Additionally, it should be noted that in initial deployment, some entities are considered centralized-by-choice for simplicity and because multiple entities are not required while the number of equipped vehicles is small. As penetration increases, these entities can proliferate and become decentralized. The entities that are expected to only have one in initial deployment include the Root CA, the Enrollment CA, the LOP, CRL Store, and CRL Broadcast.

This more complicated technical design is current as of January 2014. The technical design was provided by:

- The Crash Avoidance Metrics Partnership, a team of eight OEMs and their security experts and other partners.[234] This team developed the illustration.
- The VIIC—a consortium of OEM policy staff supporting the technical design team.

The technical design has been reviewed for its technical functionality by staff of the DOT from NHTSA, the ITS JPO, FHWA, and the Volpe Center.

1. SCMS component functions

The following discussion of SCMS functions focuses on communications and activities within the SCMS. The technical design for the SCMS includes several different operating functions that together make up the overall SCMS structure.

We note that the interactions between the components shown in Figure IX-2 are all based on machine-to-machine performance. No human judgment is involved in creation, granting, or revocation of the digital certificates. The functions are performed automatically by processors in the various V2V components, including the OBE in the vehicle. The role of personnel within the SCMS is to manage the overall system; protect and maintain the computer hardware and facilities; update software and hardware; and address unanticipated issues.

Generally, these SCMS operating functions fall into two categories: pseudonym functions and bootstrap functions. In order for the SCMS to support the security needs of the V2V system, the various SCMS functions must work together to exchange information securely and efficiently.

2. Pseudonym functions/certificates

The security design makes use of short-term digital certificates used by a vehicle's on-board equipment to authenticate and validate sent and received basic safety messages that form the foundation for V2V safety technologies. These short-term certificates contain no information about users to protect privacy, but serve as credentials that permit users to participate in the V2V

---

[234] Including security experts from ESCRYPT, Inc., CAMP, and Booz Allen Hamilton.

system. Pseudonym functions create, manage, distribute, monitor and revoke short-term certificates for vehicles. They include:

- Intermediate Certificate Authority (Intermediate CA) is an extension of the Root CA shielding it from direct access to the Internet. It can authorize other Certificate Management Entities (CMEs) (or possibly an Enrollment Certificate Authority [ECA]) using authority from the Root CA, but does not hold the same authority as the Root CA in that it cannot self-sign a certificate. The Intermediate CA provides flexibility in the system because it obviates the need for the highly protected Root CA to establish contact with every SCMS entity as they are added to the system over time. Additionally, the use of Intermediate CAs lessens the impact of an attack by maintaining protection of the Root CA.

- Linkage Authority (LA) is the entity that generates linkage values. The LA has been designed to come in pairs of two, which we refer to as LA1 and LA2. The LAs for most operations communicate only with the RA and provide values, known as linkage values, in response to a request by the RA (see below) and PCA (see below). The linkage values provide the PCA with a means to calculate a certificate ID and a mechanism to connect all short-term certificates from a specific device for ease of revocation in the event of misbehavior.

- Location Obscurer Proxy (LOP) obscures the location of OBE seeking to communicate with the SCMS functions, so that the functions are not aware of the geographic location of a specific vehicle. All communications from the OBE to the SCMS components must pass through the LOP. Additionally, the LOP may shuffle misbehavior reports that are sent by OBEs to the MA (see below) during full deployment. This function increases participant privacy but does not increase or reduce security.

- Misbehavior Authority (MA) acts as the central function to process misbehavior reports and produce and publish the certificate revocation list. It works with the PCA, RA, and LAs to acquire necessary information about a certificate to create entries to the CRL through the CRL Generator. The MA eventually may perform global misbehavior detection, involving investigations or other processes to identify levels of misbehavior in the system. The MA is not an external law enforcement function, but rather an internal SCMS function intended to detect when messages are not plausible or when there is potential malfunction or malfeasance within the system. The extent to which the CMEs share externally information generated by the MA about devices sending inaccurate or false messages – either with individuals whose credentials the system has revoked or with law enforcement – will depend on law, organizational policy, and/or contractual obligations applicable to the CMEs and their component functions.

- Pseudonym Certificate Authority (PCA) issues the short-term certificates used to ensure trust in the system. In earlier designs their lifetime was fixed at five minutes. The validity period of certificates is still on the order of "minutes" but is now a variable length of time, making them less predictable and thus harder to track. Certificates are the security credentials that authenticate messages from a device. In addition to certificate issuance,

the PCA collaborates with the MA, RA, and LAs to identify linkage values to place on the CRL if misbehavior has been detected.

- Registration Authority (RA) performs the necessary key expansions before the PCA performs the final key expansion functions. It receives certificate requests from the OBE (by way of the LOP), requests and receives linkage values from the LAs, and sends certificate requests to the PCA. It shuffles requests from multiple OBEs to prevent the PCA from correlating certificate IDs with users. It also acts as the final conduit to batching short-term certificates for distribution to the OBE. Lastly, it creates and maintains a blacklist of enrollment certificates so it will know to reject certificate renewal requests from revoked OBEs.

- Request Coordination is critical in preventing an OBE from receiving multiple batches of certificates from different RAs. The Request Coordination function coordinates activities with the RAs to ensure that certificate requests during a given time period are responded to appropriately and without duplication. Note that this function is only necessary if there is more than one RA in the SCMS. The technical process behind this function is still under development.

- Root Certificate Authority (Root CA)) is the master root for all other CAs; it is the "center of trust" of the system. It issues certificates to subordinate CAs in a hierarchical fashion, providing their authentication within the system so all other users and functions know they can be trusted. The Root CA produces a self-signed certificate (verifying its own trustworthiness) using out-of-band communications. This enables trust that can be verified between ad hoc or disparate devices because they share a common trust point. It is likely that the Root CA will operate in a separate, offline environment because compromise of this function is a catastrophic event for the security system.

- SCMS Manager is the function that will provide the policy and technical standards for the entire connected vehicle industry. Just as any large-scale industry ensures consistency and standardization of technical specifications, standard operating procedures, and other industry-wide practices such as auditing, the SCMS Manager would perform and monitor these types of activities. This can happen in a number of ways. Often in commercial industries, volunteer industry consortiums take on this role. In other industries, or in public or quasi-public industries, this role may be assumed by a regulatory or other legal or policy body. Despite the choice of how to implement a central administrative body, it is expected practice that one would be established for the SCMS. As no decisions about ownership or operation have been made, we do not advocate for public or private ownership, but include the basic functions we expect the SCMS Manager would perform in our discussions and analyses. The expectation is that the SOPs, audit standards, and other practices set by this body would then be executed and complied with by each CME individually. It is also assumed that any guidance, practices, SOPs, auditing standards, or additional industry-wide procedures would be set based on any Federal guidance or regulation. The SCMS will also remove or revoke entities that do not comply with standards or misbehave.

3. Initialization functions/enrollment certificate

The security design also includes functions that carry out the bootstrapping process, which establishes the initial connection between a motor vehicle's OBE and the SCMS. The chief functional component of this process is the Enrollment Certificate Authority that assigns a long-term enrollment certificate to each OBE. To the extent required by NHTSA or other stakeholders, it is during the bootstrap process that the SCMS can create a link between specific OBEs or production lots of OBEs and enrollment certificates that later may be used by OEMs and NHTSA to identify defective V2V equipment. The design does not indicate when bootstrapping should take place, but NHTSA has suggested that it might need to take place at the time of OBE manufacture to facilitate the level of linkage between long-term enrollment certificates and equipment production lots that NHTSA needs for enforcement purposes (e.g., to identify defective equipment).

Note that, at this time, bootstrap functions have been fairly well defined for OBEs. The process for establishing the connection between aftermarket safety devices and the SCMS has not been defined; nor will it be defined by CAMP (it will need to be defined by ASD manufacturers who will need to work with the final structure of the SCMS to determine how to do this process).

Initialization functions include:

- Certification Lab does not take part in the particular use cases [of the SCMS]. It instructs the ECA on polices and rules for issuing enrollment certificates. This is usually done when a new device is released to the market or if the SCMS Manager releases new rules and guidelines. The Enrollment CA uses information from the Certification lab to confirm that devices of the given type are entitled to an enrollment certificate. As identified in Section VI.G, details regarding the Certification and Enforcement are not currently determined.[235]

- Device Configuration Manager (DCM) is responsible for giving devices access to new trust information, such as updates to the certificates of one or more authorities, and relaying policy decisions or technical guidelines issued by the SCMS Manager. It also sends software updates to the OBEs. The DCM coordinates initial trust distribution with OBE by passing on credentials for other SCMS entities, and provides the OBE with information it needs to request short term certificates from an RA. The DCM also plays a

---

[235] At this point, the extent and level of testing that the Certification Lab will actually perform is still to be determined. The role of the labs could range from simply managing a checklist of requirements to performing extensive technical certification tests, including: device performance, FCC compliance, cryptographic testing (at the level of FIPS-140), and/or interoperability testing. The intent is that the SCMS manager, after it is created, will determine the full roles and responsibilities of the Certification Lab. Vehicle and device manufacturers may decide to rely in part on a certification lab to support the ir own certification of compliance with any relevant standards NHTSA may issue.

role in the bootstrap process by ensuring that a device is cleared to receive its enrollment certificate from the ECA. It also provides a secure channel to the ECA. There are two types of connections used from devices to the DCM: in-band and out-of-band communications. In-band communication uses the LOP, while out-of-band communication is sent directly from the OBE to the ECA by way of the DCM.

- Enrollment Certificate Authority (ECA) verifies the validity of the device type with the Certification Lab. Once verified, the ECA then produces the enrollment certificate and sends it to the OBE. Once the OBE has a valid enrollment certificate, it is able to request and receive certificates from the SCMS.

a) Unique technologies employed in the current V2V PKI security system design

Following are some of the additional technologies that are unique to the V2V PKI Security System:

b) Butterfly Keys:[236]

Butterfly keys are a novel cryptographic construction that allows a device to request an arbitrary number of certificates, each with different signing keys and each encrypted with a different encryption key, using a request that contains only one verification public key seed and one encryption public key seed and two "expansion functions" (which allows the second party to calculate an arbitrarily long sequence of statistically uncorrelated (as far as an outside observer is concerned) public keys such that only the original device knows the corresponding private keys).

Without butterfly keys, the device would have to send a unique verification key and a unique encryption key for each certificate. Thus, butterfly keys reduce the upload size of certificate requests, and allow requests to be made when there is only spotty connectivity (although they also increase the size of the certificate upload). They also reduce the work to be done by the requester to calculate the keys, thus reducing computational burden.

(1) Linkage values

To support efficient revocation, end-entity certificates contain a linkage value that is derived from cryptographic seed material. Publication of the seed is sufficient to revoke all certificates belonging to the revoked device, but without the seed an eavesdropper cannot tell which certificates belong to a particular device. (Note: the revocation process is designed such that it does not give up backward privacy.) For protection against insider attacks, the seed is the combination of two seed values produced by two Linkage Authorities; this ensures that no single organizational entity knows enough information to identify a single device. An extension to the linkage values approach allows for group revocation, so that if all devices of a particular type

---

[236] A Security Credential Management System for V2V Communications (Whyte, Weimerskirch, Kumar, and Hehn). See Docket No. NHTSA-2014-0022=

have a flaw they can be revoked with a single entry on the revocation list, while keeping group membership secret until the relevant group seed is revealed. Group revocation is considered an option besides revocation of single devices.

Linkage values and linkage authorities (LAs) are used to enable the SCMS to support seven requirements.

- There should be an efficient way of revoking all the certificates within a device
- There should be an efficient way of revoking all the certificates within a group of devices
- Certificates should not be linkable by an eavesdropper unless the owner has been revoked
- Membership to a group should not be disclosed unless that group has been revoked
- If a vehicle's security credentials are revoked, the vehicle should be identifiable going forward but its movements before it was revoked should not be trackable.[237]
- Similarly, if a group of vehicles' security credentials are revoked, a device belonging to that group should be identifiable as a member. However, it should not be possible to determine the membership to a group before the group revocation took place.
- No single entity within the system should be able to determine that two certificates belong to the same device or to the same group. An exception to this rule is the Misbehavior Authority.

If there is a requirement that no single entity within the SCMS should be able to identify a vehicle, once an LA is introduced, this requirement is no longer fulfilled. For that reason, two LAs are introduced and the information that allows for identification is split between them.

(2) Misbehavior Authority/CRL

Most SCMS functions listed above are fairly well developed. One critical function, which has not yet been fleshed out adequately for DOT to assess, is the Misbehavior Authority (MA) -- the central function responsible for processing misbehavior reports generated by OBE and producing and publishing the CRL. This list, once distributed, identifies digital certificates that are no longer valid and the OBE should no longer rely on messages from the identified digital certificates. The size of the CRL depends on the frequency of list distribution and rate of misbehavior across the vehicle fleet. On-board storage for and the costs of distributing the CRL are two major cost generators in the technical design.

The MA also will be responsible for performing global misbehavior detection, involving the collection of a sampling of misbehavior reports from OBE for purposes of detecting system-wide misbehavior and revoking misbehaving entities. Global detection processes have not yet

---

[237] Because the current design now reuses certificates, vehicles will be backwards-trackable for the period of the batch life. This design anticipates certificate batches to be valid for a week.

been defined. Should NHTSA decide to move forward with regulatory action, it will be important for NHTSA to continue to work with CAMP and perhaps other consultants to mature the misbehavior detection processes,[238] as these are critical to system integrity and have a direct relationship to system costs.

Research Need IX-1 Misbehavior Authority[239]

Research Activity:	Misbehavior Detection
Description:	Development of the processes, algorithms, reporting requirements, and data requirements for both local and global detection functions; and procedures to populate and distribute the CRL.
Target Completion:	Initial requirements completed in 2015 (draft report to NHTSA)
Current or Planned NHTSA research addressing this need:	
NHTSA is currently working with CAMP to develop Misbehavior Detection and Reporting strategies for both local and global misbehavior detection. Initial requirements that define the Misbehavior Authority functions will be complete in 2015. Validation and demonstration efforts will continue through 2016.	

4. Comparing a basic PKI to the V2V security design

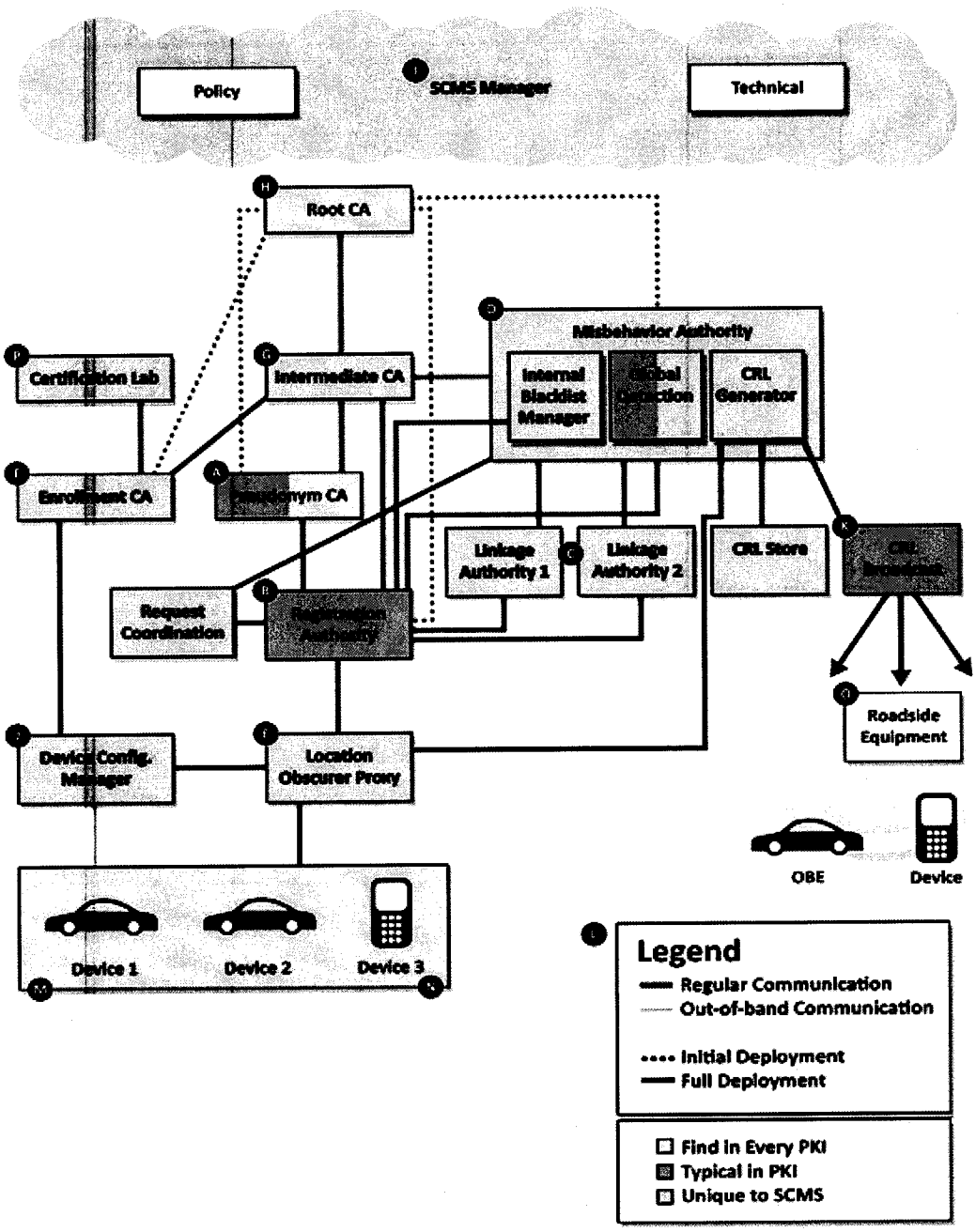
Based on the definition of these additional elements that is needed for a secure V2V environment, Figure IX-3 illustrates the differences between a "basic PKI system" that is similar to those in use today versus the V2V PKI that can deliver the highest levels of privacy protection, can be scaled to support 350M+ users, and can mitigate risks and attacks that are associated with systems in use today and in the near future.

---

[238] Some specific tasks could include evaluating: (1) how onboard diagnostics for V2V devices for local detection (malfunction) could reduce the size of the CRL; (2) how misbehavior search algorithms for global detection (malfunction and malicious) could be developed; (3) the approach and feasibility of using "epidemic distribution" to eliminate the need for a CRL; and (4) what new vulnerabilities to attack and what new enhanced data communication capability exist.

[239] Intelligent Transportation Systems: Vehicle-to-Vehicle Technologies Expected to Offer Safety Benefits, but a Variety of Deployment Challenges Exist (Nov. 2013, GAO-14-13). See www.gao.gov/assets/660/658709.pdf (last accessed Feb. 12, 2014).

Figure IX-3 V2V Security Design Comparison to a Basic PKI



The boxes in blue are the entities/functions found in every PKI. The boxes in gold are typically associated with today's PKI systems. The boxes in light green are unique to the V2V

PKI. Note that the complexity requires an overall "security credentials management system" manager. Note also that some entities/functions are split to support privacy preservation.

The additional elements added by the research team to the V2V security design are needed for the following reasons:

- The requirement to protect privacy appropriately requires a system that divides and separates some of the functionality to ensure that no one element (entity) has the ability to match records that would lead to identification of a specific driver or specific vehicle.
- There are two linkage authorities that create linkage values. Linkage values allow one entry on the CRL to revoke an entire batch of certificates, instead of having to list each certificate. This drastically reduces the size of the CRL and the communications requirement. An LA has enough information that an inside attacker can track a user. Therefore, the linkage value comes from the output of two separate linkage authorities, neither of which has enough information to track anyone. Splitting the linkage authority creates additional privacy protection but also increases organizational costs.
- The need for appropriate privacy protection has led to a greater amount of digital certificate usage; digital certificates use random identifiers that change frequently so as to lower the risk of identifying any one vehicle or driver with a particular digital certificate. The decision on how many certificates are used in a given time period or how to employ random identifiers is still to be determined (options are described but not yet decided upon). It may be a flexible choice based on type of application. Notably, allowing for different schemes might also make attacks on the system more difficult.
- Privacy considerations also have resulted in the addition of an element to obscure location coordinates when a vehicle or device communicates with the system (e.g., to request more digital certificates or to report misbehavior detected locally, around the vehicle).
- While misbehavior authorities exist in today's PKI system (typically as a part of a CA) to detect and take actions to mitigate or remove malicious behavior, the V2V PKI's MA is described as a separate and more complex entity than exists today. Not all of the described functionality of the V2V MA has been demonstrated (e.g., the use of local detection and reporting) in industry. It is, however, planned for demonstration and testing as an operational prototype that is being planned as part of the ongoing near-term CAMP research.
- The trust requirement has resulted in the design of a direct interface with a certification lab entity to verify that each type of device meet standards proving their capabilities to be trusted, secure, and interoperable.
- Request coordination is added as a function to ensure that an OBE cannot obtain multiple batches of certificates by sending requests to several RAs at the same time.

5. V2V security research conducted or underway

Table IX-2 provides a summary of the security research conducted over the past eleven years and currently underway. The research supported the development of a SCMS, explained previously, that was prototyped for the Safety Pilot Model Deployment. The different research projects built off of the previous research projects to investigate and then define the components and processes of a security system for V2V communications. The prototype SCMS that was implemented to provide Safety Pilot Model Deployment communications security will provide data that will be used to understand and evaluate the capabilities of the current prototype, and possibly indicate how it can be improved.

Table IX-2 V2V Communication Security Research

Research Project	Time Period	Research Focus
Vehicle Safety Communications (VSC)	2002-2005	Secure communications that included identifying options for: • Trust mechanisms • ID misbehaving devices • PKI architecture
Review by the National Institute of Standards and Technology (NIST)	2004	NIST reviewed the security options alternatives analysis, agreed with the security approach chosen (PKI), reviewed the emerging PKI configuration for V2V, and identified concerns that the research team would need to address as development moved forward.
Vehicle Safety Communications – Applications (VSC-A)	2006-2010	Development of high-level security design that covered: • Over-the-air performance of an authentication scheme • Identification of privacy mechanisms • Analysis of channel options for security • Refinement of the attacker model • Initial development of misbehavior detection schemes

Research Project	Time Period	Research Focus
Vehicle-to-Vehicle-Communications Security (V2V-CS)	2010-2012	Research Objectives included: • Determined security requirements and derived communication channel requirements. • Delivered a simplified initial and final deployment security model that identified the 3000/year certificate model with no infrastructure required for the first three years. • Performed a system-based risk assessment using the proposed initial and full deployment models. Assessment identified both privacy and security risks. • Began definition of the SCMS to understand the organizational and operational requirements; identified a need to research ownership/operations from a centralized versus non-centralized perspective. • This version of the SCMS formed the basis for the Safety Pilot Model Deployment prototype.
Vehicle-to-Vehicle-Interoperability, Phase 1 (V2V-I)	2010-2012	Research objectives for defining interoperability included further research into security from an operational perspective. The research covered: • Definition of a concept of operations for a V2V security; tested the operations with 200 vehicles to observe channel congestion using both cellular and DSRC. • Definition of a process of certificate management and an initial process for misbehavior detection. • Publication of design specifications on IP.com and licensing of the operational design for use in the Safety Pilot Model Deployment.
Oak Ridge National Laboratories (ONRL)	2012	Before the launch of the Safety Pilot Model Deployment, ORNL tested the prototype security system.

Research Project	Time Period	Research Focus
Safety Pilot Model Deployment (SPMD)	2012-2013	Implementation of a prototype that included: • Support for device initialization • Pre-load of certificates onto devices • Over-the-air certificate reload • Testing of the certificate revocation list • Testing of misbehavior reporting function
Vehicle-to-Vehicle-Vehicle Safety Communications Security Studies (V2V-VSCS)	2012-2014	Research is underway and includes: • Finalization of the SCMS design with a focus on simplifying and optimizing operations • Cost analysis of the SCMS with a sensitivity analysis on the assumptions associated with the current design concept. • Identification of optional methods to link batches of on-board equipment devices to enrollment certificates
V2V Interoperability Project/Phase 2 (V2V-I/Phase 2)	2012-2014	Research is underway and is focused on misbehavior detection and reporting – the algorithms and operational requirements needed to ensure that this function works under real-world conditions that will lead to development of a deployment use case.
Independent Evaluation of V2V Security System Design	2014-2015	To better understand the state of the current design, the DOT needs an independent entity's assessment to inform the DOT of the status of the design and provide a basis for future policy and technical decisions.

6. Overall application of cryptography in V2V communications

The security approach for V2V system is based predominantly on use of a public key infrastructure to support trusted messaging, feasible operations, and appropriate privacy protection. Other forms of security—symmetric encryption, physical security and system controls, organizational security, and legal deterrence policies are incorporated judiciously throughout the system. The decisions on where and how to apply security have been made with safety as the highest priority, and a balance between protecting privacy appropriately, latency and bandwidth concerns, preliminary costs, flexibility, and non-repudiation. Additionally, all of

the cryptographic methods are expected to provide a security level of at least 128 bits and are NIST compliant.[240]

Below is a high level but technical summary of how these various mechanisms are built and applied at key risk points throughout the system:

- **Digital Certificates:** Are based on the Elliptic Curve Qu-Vanstone Implicit Certificate Scheme[241]; and IEEE Standard 1609.2-2013[242] is used for generating digital certificates. Keys with the certificates are generated using the "butterfly keys" scheme, which is not yet standardized.
- **Digital Signatures:** Are based on the Elliptic Curve Digital Signature Algorithm from the Digital Signature Standard that is used for digitally signing messages.[243] Note that NIST requires the use of a hash function (SHA-256[244]) during ECDSA signature generation, for security purposes. The CAMP design follows this principle.
- **Asymmetric Encryption:** Elliptic Curve Integrated Encryption Scheme as specified in IEEE Standard 1363a-2004[245] is used for asymmetric encryption. In the CAMP design, ECIES is used only to encrypt a symmetric key, which is then used for encrypting a message to the receiver using symmetric encryption (as described below). ECIES internally makes use of keyed-hash message authentication codes.[246]

---

[240] Approved Security Functions for FIPS 140-2 (May 30, 2012, Federal Information Processing Standard Publication, Annex A) at http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexa.pdf (last accessed Jan. 30, 2014); and Recommendation for Pair-Wise Key Establishment Schemes using Discrete Logarithm Cryptography, Revised (Mar. 2007, NIST Special Publication 800-56A) at http://csrc.nist.gov/groups/ST/toolkit/documents/SP800-56Arev1_3-8-07.pdf (last accessed Jan. 30, 2014).

[241] As specified in the Certicom Research, see:

- Standard for Efficient Cryptography (SEC) 4: Elliptic Curve Cryptography, version 2.0., (Certicom Research, May 21, 2009) at www.secg.org/download/aid-780/sec1-v2.pdf (last accessed Jan. 30, 2014).
- SEC 4: Elliptic Curve Qu-Vanstone Implicit Certificate Scheme (ECQV), version 1.0. (Certicom Research, Jan. 24, 2013) at www.secg.org/download/aid-796/sec4-1.0.pdf (last accessed Jan. 30, 2014).

[242] Wireless Access in Vehicular Environments: Security Services for Applications and Management Messages (IEEE Std. 1609.2-2013) at http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6509896&queryText%3D1609.2 (last accessed Jan. 30, 2014).

[243] Digital Signature Standards (DSS) (NIST, FIPS PUB 186-4, Jul. 2013) at http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf (last accessed Jan. 30, 2014).

[244] Secure Hash Standard (SHS) (Mar. 2012, NIST, FIPS 180-4,) at http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf (last accessed Jan. 30, 2014). For a description of SHA-256, *see* http://csrc.nist.gov/groups/STM/cavp/documents/shs/sha256-384-512.pdf (last accessed Jan. 29, 2014).

[245] Standard Specification for Public-Key Cryptography-Amendment 1: Additional Techniques (IEEE Std. 1363a-2004,) at http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=1335427&queryText%3DIEEE+Std.+1363a-2004 (last accessed Jan. 30, 2014).

[246] The Keyed-Hash Message Authentication Code (HMAC) (2008, NIST, FIPS PUB 198-1) at http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf (last accessed Jan. 30, 2014).

- **Symmetric data encryption**: Symmetric data encryption is expected to be used for two separate purposes within the SCMS. The first purpose, to protect internal SCMS entity communications, has not yet been determined. Symmetric data encryption is likely to be used because it is more efficient than using asymmetric data encryption, for this purpose. But the public-private key pair (asymmetric) would be used to distribute the symmetric keys (periodically changed).

The second purpose is to provide a one-way compression of the linkage seeds to convert them into the pre-linkage values that are sent to the RA. It uses a keyed hash that offers proof of the legitimacy of the linkage authority that created them.

In both cases, the design calls for using the Advanced Encryption Standard (AES)-128.

- **Linkage Values:** Are generated using SHA-256 and using AES in raw[247] mode as input to the one-way compression that creates the keyed hash that conceals the linkage seeds (as described above).[248] Counter with CBC-MAC (CCM) mode"[249] is used to randomize the initial AES encryption and provide authentication.

Uses of these different cryptographic applications include:

- **Basic Safety Message**: Digital signatures only are used; the digital certificates that a vehicle receives from the SCMS are also attached to BSMs for verification purposes. The receiver trusts the message if it can validate the certificate.
- **Communications between vehicles and the SCMS**: Asymmetric encryption is used for confidentiality when a devices needs to reach a component of the SCMS. Digital signatures are added to show that the request is coming from a valid device. Examples include:
    - To reach the RA or the MA with a certificate request or misbehavior report, a device uses asymmetric encryption to encrypt the content for the RA or the MA.
    - To show that the certificate request is valid, the device creates a signature using the private key corresponding to the public key in the enrollment certificate.
    - To show that a misbehavior report is valid, the device creates a signature using the private key corresponding to the public key in a currently valid pseudonym certificate before sending the signed content.

---

[247] Also known as Electronic Codebook or ECB mode.
[248] As specified in: Recommendation for Block Cipher Modes of Operation (2001, NIST Special Pub. 800-38C).
[249] Recommendation for Block Cipher Modes of Operation (2001, NIST Special Publication 800-38C) at http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf (last accessed Jan. 30, 2014). Also see the CCM Mode for Authentication and Confidentiality (2004, N.W. Group) and Counter with CBC-MAC (CCM) (Sept. 2003) both at http://tools.ietf.org/html/rfc3610 (last accessed Jan. 30, 2014).

- **Communications inside the SCMS (entity to entity)**: For performance reasons, communications between the entities use symmetric encryption together with the message authentication code (MAC). The symmetric encryption provides confidentiality, and the MAC provides integrity. Together, they provide authenticity but not non-repudiation (i.e., one entity cannot tell which of the two communicating parties generated the MAC). As the SCMS separates ownership (power) and data, non-repudiation becomes less of an issue. The only exception is the communication with the MA. Here, non-repudiation is required to make sure that a request really came from the MA and was not staged by the other SCMS entity. The MA is the only entity that needs to digitally sign its requests (as opposed to using the MAC); and only during misbehavior investigations. Note the keys for symmetric encryption will be distributed to entities within the SCMS using their public-private key pairs (that is, in asymmetrically encrypted messages).
- **Certificates for vehicles and SCMS entities**: Digital certificates are used and include the linkage values described above.

7. Additional information on the current V2V security system design and research

As evidenced by the research, the current V2V security system has been developed through a set of highly technical, incremental decisions. Along the way, outside review by NIST, Oak Ridge National Laboratories, and the DOT modal partners in FHWA, FTA, and the Volpe Center have questioned decisions, highlighted concerns, and discussed/analyzed new options.

When the research results are viewed holistically, the following statements can be made about the system and accomplishments to date:

- DOT and its partners have developed a leading-edge approach to communication security, one that will enable trusted messaging, feasible operations, and preserve user privacy appropriately.
- The approach to security is based predominantly on proven cryptographic methods. Standards are employed that are tailored specifically for these security purposes; they are industry-consensus standards that are being harmonized with Europeans at the ISO[250] level.
- A working prototype has been built that proves that the basic, fundamental operations are feasible in a real world environment.
- An operational and organizational structure (architecture) is being designed that is relatively stable. Most elements are well defined – even to the point of identifying number of personnel, number of servers, hardware, etc. But there are new entities that still need definition of functions and processes.

---

[250] ISO is the International Organization for Standardization.

Models show SCMS requirements for resources[251] and for bandwidth are relatively modest even when scaled up to full deployment.[252] While the SCMS will be unprecedented in scale for a PKI system, it is not remarkable compared to existing IT systems. First year estimates for a few million equipped vehicles (equivalent to only a few percent penetration) indicate the need for approximately 30 high-end computers (processors/servers) and roughly 4500 other pieces of equipment like disk drives, monitors, keyboards, personal computers, etc. distributed across perhaps 40 facilities. Year 25 estimates for ~300 million equipped vehicles, (penetration above 95 percent) indicate the need for roughly 550 high-end computers and 29,000 other pieces of equipment distributed across perhaps 95 facilities. This covers almost all traffic over the entire country. Note the specific estimates are rough and preliminary but provide a good ballpark understanding of the scale. Data throughputs between entities are estimated at a tiny fraction of current data flows for video entertainment, for example.[253]

- European regulators and industry are using a very similar approach despite focusing on a different set of system objectives—mobility and opt-in applications. They have noted that they will likely adopt practices from the U.S. design, once finalized, when they look to implement V2V safety applications. There is a movement to harmonize on security policies at an international level.
- Strength/Validity/Break-ability of the design:
  - The design incorporates digital signature algorithms and hash algorithms that are NIST compliant and predicted to be strong until sometime in the future. (ECDSA-256 is expected to be un-breakable for another 20 years.)
  - Some initial work has been conducted with the prototype system in Safety Pilot Model Deployment to test the system to see where vulnerabilities exist. Some were found as "back-door holes" associated with the system operator and with devices. These tests have formed lessons learned that are informing the development of certification processes for devices, and are anticipated to be incorporated into standard operating procedures, deployment guidance, and policies (including within the new RSE specification).
  - Planned penetration testing will provide insight into the reliability and resiliency of the design.

[251] Including such resources as hardware, software, energy/power, and personnel.

- Notably, costs for *breaking* the key element of this security approach --ECDSA encryption-- is estimated to be very high by security experts[254]

Research Need IX-2 Cryptographic flexibility

Research Activity:	Independent Evaluation of Vehicle-to-Vehicle Security Design
Description:	The chosen cryptographic algorithms are estimated to be resilient against brute force attack for a few decades with some susceptibility through an unanticipated weakness. In the future new algorithms could enable better performance but may require redesign of functions or operations within the SCMS. Research is needed to determine if and how the existing SCMS and overall security solution design should change to build this flexibility or modularity into the system.
Target Completion:	2015 (draft report to NHTSA)
Current or Planned NHTSA research addressing this need:	
NHTSA will initiate an Independent Evaluation of the Vehicle-to-Vehicle Security Design in FY14 (Research Need IX-3) that will include an assessment of the design to support a cryptographic algorithm change.	

C. Overview of system integrity and management

Generally speaking, "system integrity" is defined as the state of operating within the limitations of mandated (not necessarily by government) or prescribed operational and technical parameters, performing its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.[255] "System management," in turn, is defined as execution of the set of functions required to support a communications network and the individuals, activities, or organizations that are the network's end users. For end users, such functions may include registering, verifying, enrolling, credentialing, billing, or revoking credentials. For the network, such functions may include controlling, planning, allocating, deploying, coordinating, and monitoring the resources of the network; initial network planning, frequency allocation, predetermined traffic routing to support load balancing, cryptographic key distribution authorization, configuration management, fault management, security management, performance management, and accounting management. Such tasks typically do not include provision of end user equipment.[256] In this case the functions support operations of the Security Certificate Management System for V2V communications.

---

[254] Vehicle Safety Communications-Applications: Final Report, Appendix Volume 3, at F-45. See www.nhtsa.gov/Research/Crash+Avoidance/Office+of+Crash+Avoidance+Research+Technical+Publications (last accessed Jan. 15, 2014).

[255] Federal Standard 1037C (General Services Administration document in support of MIL-STD-188). See www.its.bldrdoc.gov/fs-1037/fs-1037c.htm (last accessed Jan. 30, 2014).

[256] Id.

As used in this discussion, the terms "system integrity" and "system management" together are intended to encompass all of the functions, activities, and organizations that play a role in ensuring the security and trustworthiness of V2V communications and the privacy of system users based on the public key infrastructure (PKI) framework and technical design produced through joint research by DOT and CAMP. The term "user" refers to users of devices, whether original equipment or aftermarket.

The technical requirements for the current V2V communications security design require a SCMS made up of individual Certificate Management Entities (CMEs) to administer the security functions supporting the connected vehicle system. The term "CME owner/operator" refers to the entities that will have legal and operational control over individual organizations that run SCMS functions.

To be viable from NHTSA's standpoint, the SCMS, as a whole, and the individual CMEs must satisfy certain key principles established by DOT in 2012:[257]

- Security and ability to detect and respond to attacks – the system must incorporate functions and processes to protect and monitor the systems. These functions must be able to identify anomalies and take action if anomalies present a threat to system operation.
- Privacy protection at the appropriate level – the system, through design and procedure, needs to appropriately protect the identity and daily activity of users of the system.
- Support of transportation safety – the system must contribute to supporting the safety need.
- Cost-effectiveness – the cost to operate the system must be balanced to the benefit attributed to the system.
- Extensibility across applications on a national scale – the system must be expandable to support nationwide development of V2V technology.

Both system integrity and system management are critical pre-conditions for safe, reliable V2V communications and appropriate privacy protection for users in a V2V-enabled environment. System integrity, by maintaining the state of the SCMS operation within established performance parameters and providing security for V2V messaging without deliberate or unintentional unauthorized interference, creates the environment of trust required for cooperative safety messaging. Users of the system must be able to trust the content of the messages received from other users. System integrity forms the critical basis for that essential

---

[257] Principles for a Connected Vehicle Environment Discussion Document (DOT, April 18, 2012). See www.its.dot.gov/connected_vehicle/principles_connectedvehicle_environment.htm (last accessed Jan. 30, 2014).

trust. At the same time, system management facilitates and enables system integrity by performing the set of technical and organizational functions that provide the foundation for system integrity.

Elements key to establishing system integrity and management include:

- The System's Technical Design,
- System Functions,
- System Organization,
- System Ownership and Operation,
- Enforcement of System Integrity and Management, and
- System Governance.

Some of these key elements were discussed in detail in Section IX.B – namely, system technical design and system functions – and therefore will not be covered again in this section. In the following sections, we address the remaining key system elements in turn.

Please note that a majority of the content of the System Integrity and Management and subsequent governance discussions are based on comprehensive SCMS research by Booz Allen Hamilton, detailed in the BAH report entitled *Security Credentials Management System (SCMS) Design and Analysis for the Connected Vehicle System*, dated December 27, 2013.[258]

1. Key elements of system integrity and management

Section IX.B describes a technical security system design for initial and full deployment in detail. For this reason, the discussion below provides only a brief, high-level summary of the aspects of the technical design necessary to support and put in context the subsequent policy discussion of System Organization, Ownership and Operation, and Governance. Preliminary system costs are addressed in detail in Section XI.

The SCMS technical design reflects the processes associated with certificate production, distribution, and revocation. Figure IX-4 above illustrates how the SCMS functions interact with each other and with OBE.

As explained in Section IX.B, the SCMS technical design uses a PKI framework to achieve the security goals related to establishing trust among users. Using PKI cryptography allows for creation and management of digital certificates that certify the sources of messages,

---

[258] Security Credentials Management System (SCMS) Design and Analysis for the Connected Vehicle System (Booz Allen Hamilton, Inc., Dec. 27, 2013). [Hereafter, "BAH SCMS Design and Analysis Report"]. See Docket No. NHTSA-2014-0022.

enabling users to trust one another and the system as a whole.[259] The use of digital certificates to establish trust among users forms the conceptual basis for the SCMS technical design.

At DOT's request, CAMP researched and developed a phased security system deployment design featuring "initial deployment" (for up to 3 years) and "full deployment." The key difference between the two is that not all SCMS functions will be available during initial deployment, and there will be no communications between OBE and the SCMS. This approach is intended to bring users into the V2V system gradually as connectivity evolves and as some of the more complex SCMS functions are developed further and readied for deployment. During initial deployment, OBE and Aftermarket devices will download and use three-year batches of certificates.

CAMP has put forth 2 options for size of certificate batches and related usage:

- Option 1: Three-year reusable, non-overlapping five-minute certificates
- Option 2: Three-year batches of reusable, overlapping,[260] five minute certificates valid for one week

CAMP compared the options by assessing implications for privacy,[261] security against Sybil attacks,[262] and certificate storage and generation costs. On the basis of its analysis, CAMP found Option 2 as technically preferable to Option 1, primarily because Option 2 protects against retrospective linkability of certificates better than Option 1. This characteristic of Option 2 makes identification of vehicles or their drivers harder and, therefore, in CAMP's view, provides less risk to individual privacy. DOT continues to work with CAMP to assess the viability and advantages/drawbacks of each option.

The security system design contemplates a hierarchical PKI containing a Root Certificate Authority and multiple Intermediate Certificate Authorities. The Root CA is the master root for all other CAs; it is the "center of trust" of the system.[263] It will issue digital CA certificates to subordinate CAs in a hierarchical fashion for use in their authentication within the SCMS so that

---

[259] An Approach to Communications Security for a Communications Data Delivery System for V2V/V2I Safety: Technical Description and Identification of Policy and Institutional Issues (Nov. 2011, DOT, OST-R, JPO, White Paper). See http://ntl.bts.gov/lib/43000/43500/43513/FHWA-JPO-11-130_FINAL_Comm_Security_Approach_11_07_11.pdf (last accessed Jan. 30, 2014).

[260] "Overlapping" means a certificate can be used at any time during the validity period – continuously until it expires.

[261] How well each option's specifications prevent a user from being tracked, concurrently or retrospectively – which is promoted by using certificates for a limited time without reuse.

[262] A Sybil attack involves an attacker using certificates to create the illusion of multiple cars on the road, which can be dangerous to OBEs – prevented by allowing only one certificate to be valid at a given time.

[263] CAMP, Task 5 Extension: Security Credentials Management System (Draft 0.5, April 2013). See Docket No. NHTSA-2014-0022

all other users and functions know they can be trusted. The Root CA is the only entity that can self-sign a certificate – the CAs cannot. All trust for the system components and users is inherited and delegated from the Root CA through certificate issuance.

The basic premise is that just as vehicles and infrastructure in the system need to be "trusted" through the use of short-term certificates that accompany V2V messages, the SCMS functions need to be "trusted" by the vehicles or infrastructure when receiving certificate batches from that SCMS function. SCMS functions also need to trust one another. For these reasons, most SCMS functions receive their own digital certificates, referred to as "CME certificates." An OBE will examine the CME certificate of any digitally signed message it receives before it accepts the message as valid to ensure:

- The certificate has not expired,
- The CME that issues the certificate is trusted, and
- The certificate is not listed on a Certificate Revocation List.

CME certificates do not need to be short-lived like the 5-minute certificates intended for the OBE, as trip tracking is not a risk for the SCMS function, because privacy is not an issue there. Additionally, not all SCMS functions require CME certificates.

DOT brought Booz Allen Hamilton on board as its consultant to: (1) assess the extent to which the evolving security design satisfies mission-based needs and DOT's Principles for a Connected Vehicle Environment, described above; and (2) develop and analyze different organizational models for the SCMS and its component CME entities based on the limited and full deployment scenarios.[264] As part of this work, BAH analyzed alternative CME models, taking into account the need for security and appropriate user privacy. BAH also identified and evaluated options related to parts of the security system not fully developed, as well as estimated preliminary costs associated with the current design. Finally, BAH identified topic areas for which further exploration is needed prior to SCMS implementation. The agency agrees that these areas represent additional research that will be needed to move forward with an SCMS.

---

[264] BAH SCMS Design and Analysis Report.

Research Need IX-3 Independent Security Design Assessment[265]

Research Activity:	Independent Evaluation of Vehicle-to-Vehicle Security Design
Description:	Independent evaluation of CAMP/USDOT security design to assess alignment with Government business needs, identify minimum requirements, assess the security designs ability to support trusted messages and appropriately protect privacy, identify and remove misbehaving devices, and be flexible enough to support future upgrades.
Target Completion:	2015 (draft report to NHTSA)

Current or Planned NHTSA research addressing this need:
The Independent Evaluation of the Vehicle-to-Vehicle Security Design will be a comprehensive evaluation of the design to identify minimum requirements, assess if and or how USDOT requirement are or can be incorporated into the design, assess the design's security capacity, identify security threats the design currently addresses, and identify possible modification to improve the design.

Whereas the discussion of SCMS functions in Section IX.B focused on activities and communications within the SCMS, the current section discusses the DOT research performed by BAH (with input from CAMP/VIIC) on development and analysis of SCMS organizational options. The purpose of BAH's research was to generate organizational options for the SCMS by grouping the SCMS functions in CAMP's design into legally/administratively distinct entities, in order to enable secure and efficient communications and protect privacy appropriately while minimizing cost. BAH's analysis of the organizational options for the SCMS, detailed below, focused primarily on organizational connections and separations, as well as the closely-related process of characterizing functions as "central" or "non-central" (which is intimately tied to the issue of system ownership and operation). It also examined the cost, security risk, and/or operational/policy implications of the different SCMS models.

BAH began by identifying multiple organizational models that, together, captured all possible configurations of the SCMS functions identified by CAMP. DOT initially selected a small number of these organizational models for BAH to flesh out. As CAMP's technical design evolved, DOT instructed BAH to reconfigure the models being fleshed out to reflect additional SCMS functions added to the SCMS design by CAMP, as well as CAMP's new categorization of functions as either "central" or "non-central." Based on its independent PKI research, as well as

---

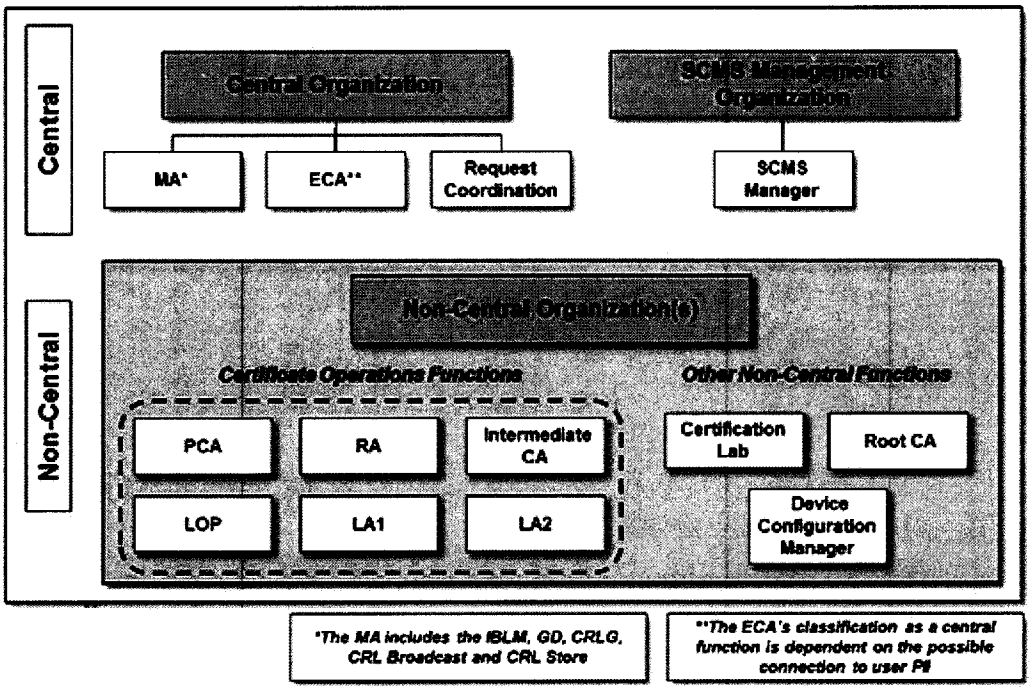
[265] Intelligent Transportation Systems: Vehicle-to-Vehicle Technologies Expected to Offer Safety Benefits, but a Variety of Deployment Challenges Exist (Nov. 2013, GAO-14-13). See www.gao.gov/assets/660/658709.pdf (last accessed Feb. 12, 2014).

new insights into the security design communicated by CAMP, BAH then simplified the initial organizational design proposed by CAMP to remove certain organizational separations of functions that BAH determined were not necessary for security or privacy reasons. CAMP/VIIC subsequently agreed that several pseudonym functions (e.g., linkage authorities and RA), initially viewed by CAMP/VIIC as needing to be housed in separate legal/administrative entities, may reside in the same CME organization without compromising privacy or security requirements.

Ultimately, the organization of the SCMS– the final grouping of functions and estimates of any efficiencies -- will be controlled by the organization(s) that manage the SCMS and own and operate the component CMEs. However, NHTSA anticipates being able to influence the organization and operation of the SCMS (and thereby ensure adequate separation to assure secure, privacy appropriate V2V communications) through agreement or MOU with the SCMS Manager or through participation on an SCMS "governance board," as discussed further in the governance section below.

BAH's SCMS organizational model/analysis is based on CAMP's latest SCMS technical design and represents BAH's perspective of how functions within the SCMS may be grouped.

Figure IX-4 Security Certificate Management System Organizational Model



DOT/BAH and CAMP/VIIC have somewhat different perspectives on whether certain functions with the SCMS should be categorized as "central" (functions that need to be owned and operated by a single legal entity) or "non-central" (functions that may be owned and

operated by multiple legal entities). The issue of whether a function is central or non-central has significant policy implications both for SCMS Organization and for SCMS Ownership/Operation.

CAMP/VIIC has taken the position that the SCMS Manager, Request Coordination and MA functions all are intrinsically central. CAMP/VIIC also uses the term "central-by-choice" to refer to functions that *can* be owned and operated by more than one legal entity, but for simplicity reside in only one operator/owner. It is our understanding that CAMP believes that the same organization(s) that run non-central functions *also* can operate central functions. CAMP's technical design for the SCMS reflects their division of functions into "intrinsically central," "central by choice," and "non-central."

By contrast, focusing more on concepts of organizational modeling rather than on technical requirements, and analyzing from a legal/administrative perspective, BAH does not distinguish between "central-by-choice" and "intrinsically central." Instead, it defines "central functions" as those that must be owned and/or operated by a single organization *that does not own or operate any non-central functions*. BAH defines "non-central functions" as those that may be owned and operated by multiple distinct organizations. BAH's organizational model reflects its determination, based on conflict of interest principles and PKI best practices, that organizations that own own/operate central functions (e.g., the SCMS Manager, ECA, MA) should not own/operate non-central functions (such as the PCA, RA, LAs, Intermediate CA, LOP, Root CA, certification lab or DCM).[266]

CAMP/VIIC has classified the ECA as non-central, while BAH would classify it as central if the ECA is involved in collecting any personally-identifying information that could link a long-term enrollment certificate to short-term certificates used to authenticate V2V messages. This is probably due to the fact that CAMP's technical security design, in order to achieve the CAMP/VIIC's stated privacy and consumer acceptance goal of "end-to-end" anonymity, does not contemplate collection of any information that could link or be used to link short-term certificates to an OBE, vehicle or driver. That being said, DOT specifically instructed BAH to incorporate into its organizational models various options for linking short-term digital certificates to production runs of OBE, OBE, VINs, and drivers for purposes of identifying, investigating, and/or recalling potentially-defective V2V equipment.. CAMP also has agreed to incorporate into its work technical and organizational options, respectively, that would enable collection of information to permit such linkage for these purposes

Currently, NHTSA believes that collection of information linking long-term enrollment certificates to production lots of V2V equipment in connection with the bootstrapping process

---

[266] BAH SCMS Design and Analysis Report, Chapter 5 at 45.

will satisfy its mission-based information needs (i.e., investigation and recall of defective vehicles or V2V equipment). This would require some of the CME organizations to work together in a way not currently contemplated by CAMP's latest technical security design, to combine information that will link short-term certificates implicated in certain misbehavior reports and processes (and therefore emanating from potentially-defective V2V OBE) to enrollment/long-term certificates.

As part of its work for DOT, CAMP/VIIC are exploring options for specific processes to accomplish this end. Once CAMP proposes such options, NHTSA will work with CAMP and VIIC to determine whether the proposed collection and storage processes meet the agency's informational needs and, if so, the extent to which the process options implicate designation of the ECA as central or non-central. BAH has emphasized that should linkage with individually-identifying information take place, the information collected should exist only within a central ECA and should be separated from the Root CA to decrease the possibility of a malfeasant insider linking identifying information in the enrollment certificates with the short-term certificates used for V2V communications. The agency will analyze the extent to which organizational separation of the CME functions required to link enrollment certificates to production lots will mitigate any privacy risks stemming from such linkage as part of its comprehensive privacy risk analysis, discussed in Section VIII.B.

Organizational separation of functions is an example of a policy control often used to mitigate privacy risks in PKI systems – but such separations come with increased costs and may negatively impact the system's ability to identify and revoke the credentials of misbehaving devices. Ultimately, other functions may be co-located within the same SCMS component organization. However, grouping of SCMS functions and any resulting efficiencies/risk trade-offs will depend, in large part, on the system's ownership and operational structure, as well as system governance, and on the preferences of the entity or entities that own and operate the SCMS Manager and CME component entities.

The SCMS Manager is intended to serve as the entity that provides system management, primarily by enforcing and auditing compliance with uniform technical and policy standards and guidance for the SCMS system-wide. The uniform standards/guidance will need to establish and ensure consistency, effectiveness, interoperability, and appropriate security and privacy protection across the CMEs to facilitate necessary communications, sharing of information, and operational connections. The SCMS Manager will need to have mechanisms to ensure that all CME entities have policies, practices, technologies, and communications consistent with system-wide standards and guidance. The SCMS Manager may (but need not) be the body that develops the standards, guidance, or policies applicable system-wide, and would be the entity charged

with overseeing standards and policy compliance by the CME entities that, together with the SCMS Manager, make up the SCMS. Technical standards and guidance exist applicable to PKI industry-wide that likely will form the basis for many of the policies and procedures applicable across the SCMS.[267]

2. SCMS ownership and operation

SCMS ownership and operation is inextricably linked to SCMS governance, discussed in more depth below. In essence, there are three basic organizational models that apply *both* to SCMS ownership and operation and to SCMS governance: public, public-private and private. Due to the lack of Federal funding available to support an SCMS, DOT research to date has focused on the likelihood of private ownership and operation of the SCMS "industry," with governance being largely "self-governance" by private industry participants and stakeholders, except to the extent that operational requirements may stem from Federal law, regulation, contract or agreement.

As discussed in Section XI below, our preliminary cost estimates for a V2V system include the assumption that a private entity would own and operate the SCMS, and impose costs that would be covered by increases in the purchase price of new vehicles. For this reason, the SCMS organizational structure discussed in the prior section – the organizational separations and groupings of functions into legally/administratively distinct CME component entities -- may not necessarily be realized in any private SCMS eventually implemented to support connected vehicle communications. In the context of a private SCMS "industry," the organizational structure and operation of the SCMS will be determined by private owners and operators of CME components, under the oversight of an SCMS Manager (ideally an industry-wide coalition of CME owners and other stakeholder representatives who, together, agree on the terms of self-governance and system-wide SCMS policies).

DOT and its consultants have identified numerous potential private and public owners and operators who could play a role in running one or more of the SCMS functions. However, at this point in time, the extent to which any entity would be interested in running one or more SCMS functions remains unclear. The list includes:

- OEMs,
- Industry groups (e.g., the American Association of Motor Vehicle, Administrators (AAMVA)),
- PKI Security organizations and companies,
- Telecommunications companies,

---

[267] BAH SCMS Design and Analysis Report, at 29.

- State and local government agencies, and
- Academic institutions.

BAH pointed out in its research that ownership and operation of non-central functions could take different forms. While there are advantages of having different owners (e.g., individual OEMs) oversee large CMEs comprised of all non-central functions, the BAH team has suggested that running such an overarching CME should not be a *condition* of ownership. Thus, for example, an entity that wants to own and operate one or more LOPs should not necessarily be required to operate *all* of the other non-central functions.[268]

BAH's research also has emphasized that qualifications for ownership and/or operation of non-central functions may be very different from those required for ownership and/or operation of central functions. For example, due to the critical importance of the security and effectiveness of operation of the Root CA, BAH has suggested that the owner/operator of this function should have expertise in PKI technology appropriate for the role. BAH also has explored the possibility that the OEMs could have a role in the system manager function/organization, but in a manner that is legally distinct from ownership/operation of the non-central functions that individual OEMs might want to own and operate (e.g., the RA functions involving interface with their clients). Shared governance by the OEMs, as through a legally/administratively distinct coalition or body, could be consistent with BAH's recommendations for separation of central and non-central SCMS ownership/operation, and would have distinct advantages, such as assurance of uniformity in standards and interoperability of equipment.[269]

Should the agency move forward with regulatory action, DOT will need to work with CAMP, BAH and potentially others (consultants, interested potential CME owners and stakeholders) to perform additional analysis of ownership/operation requirements and candidates, and to address the following questions:

- Who will set the various standards, policies, procedures, auditing processes, and other related industry-wide processes?
- Who are the appropriate candidates for ownership for central and non-central functions?
- What are the conditions of ownership?
- Can multiple central functions be combined or operated by the same organization
- To what extent should SCMS owners be required to support V2V and V2X needs as the system connected vehicle environment expands?

---

[268] BAH SCMS Design and Analysis Report, at 45. See Docket No. NHTSA-2014-0022
[269] BAH SCMS Design and Analysis Report, at 45.

3. "Enforcement" of system integrity/SCMS manager

Enforcement of "system integrity" is closely related to the general area of SCMS governance. In the context of CAMP's SCMS technical design, envisioned by NHTSA as a privately owned and operated "industry," a private SCMS will enforce system integrity within the SCMS through self-regulation and binding agreements with the entities agreeing to be regulated. Organizationally, enforcement is the primary responsibility of the SCMS Manager. The SCMS Manager provides critical system management by enforcing and auditing compliance with uniform technical and policy standards and guidance applicable system-wide. The uniform standards/guidance will need to establish and ensure consistency, effectiveness, interoperability and appropriate privacy protection across the CMEs to facilitate necessary communications, sharing of information, and operational connections, and most likely will be based in large part on existing technical standards applicable to PKI systems.

4. "Enforcement" of system integrity/Federal role

In the context of the SCMS technical design, envisioned as a privately owned and operated "industry," we view the Federal role by NHTSA in "enforcing" or otherwise ensuring system integrity as fairly limited. Primarily, the agency would perform its traditional regulatory role. In addition, NHTSA's agreement with the CME entities that constitute the SCMS, or the SCMS Manager on behalf of those CMEs (if they are inclined to sign an agreement), could provide supplemental enforcement or oversight mechanisms, consistent with our authority. Other Federal entities also likely will have some "enforcement" jurisdiction over aspects of system integrity, including the jurisdiction of the Federal Trade Commission over compliance by the SCMS entities that interact with end users with their own privacy policies.

Consequently, the specific elements of Federal "enforcement" relating to system integrity would include:

- NHTSA compliance and enforcement of the security aspects of a potential FMVSS via development of compliance testing procedures and enforcement via the manufacturer's self-certification and NHTSA selection of some items for testing in relation to devices identified as motor vehicle equipment;
- NHTSA ODI investigation and recall of potentially defective V2V equipment;
- NHTSA enforcement of Agreements with SCMS Manager (and SCMS entities), if the SCMS is willing to enter into an agreement with NHTSA;
- FTC enforcement of the terms of privacy policies against SCMS entities interfacing with end users; and
- FCC enforcement of use of spectrum.

Other than as noted here, neither DOT nor NHTSA would assume any new "enforcement" responsibilities in the context of the envisioned privately-owned and self-

regulated PKI "industry" that could support V2V communications in a secure, efficient privacy-appropriate way with minimal Federal involvement.

D. System governance and why it is important

Although heavily dependent on context, the term "governance" generally refers to the way rules are established, implemented, and enforced. Governance can mean formal regulatory oversight by a Federal, State, or local governmental entity. NHTSA's issuance and enforcement of FMVSSs under the Safety Act is an example of governance by a Federal entity. However, governance does not always require the participation of a "government" (i.e., a geo-political entity). In the context of corporate entities, governance typically refers to consistent management, cohesive policies, guidance, processes, and decision-rights for given areas of responsibility.

Deployment of V2V technologies will require governance of a wide range of complex functions and legal issues. For purposes of this discussion, we have divided these functions and issues into two categories: those outside the purview of the SCMS, and those inside its purview. Areas of governance falling outside of the SCMS (most notably, performance standards and requirements, FCC certification requirements, device communications interoperability, and spectrum allocation and management) are addressed substantively elsewhere in this decision paper. For this reason, the following discussion of "system governance" focuses solely on the important policy area of governance of the security system required to support the SCMS.

As used in this discussion:

- **"SCMS System"** is defined as all the needed functions associated with security certificate management for the connected vehicle system – from the SCMS Manager down to the individual functions and the component CME entities in which they may reside.

- **"System Governance"** refers to the body or set of bodies/entities that determine standards, policies, compliance requirements, and expectations for all organizations that have a role to play in certificate management as part of the SCMS that will be needed to support deployment of V2V technologies.

System governance encompasses:

- How decisions are made about various policies, standards, requirements, and practices;

- Who has the authority to mandate and enforce compliance with the policies, standards, and industry requirements;

- Who makes up the overseeing financial, legal, management, and executive operations of the entities in the SCMS;

- How various entities interact with each other;
- How the system addresses privacy issues;
- How risk and liability are allocated across the organizations;
- Who will own the intellectual property (data and software) of the system; and
- How the system's intellectual property will be licensed or otherwise allocated among and between internal and external entities.

The SCMS technical design and related work of the VIIC call for an SCMS made up of a central SCMS Manager and various CME component organizations together performing all functions required for certificate management. As discussed in detail above, the SCMS Manager will define and oversee certain standards, policies, procedures, and operational practices applicable to the SCMS component entities. The potential scope or extent of authority and operations of the SCMS Manager are still under development, but as in all industries, there are three fundamental options for organizational structure from which to choose for SCMS industry governance (the same three apply to the inextricably-related issue of SCMS ownership and operation):

- **Public**: governance structure determined and administered by the government, either directly or indirectly (as via a contractor)
- **Public-Private Partnership (PPP)**: any organizational structure authorized by law within the range between a purely government organization and a purely private organization, established and administered in accordance with the authorizing partnership or similar document (typically a grant, cooperative agreement or other agreement)
- **Private**: governance structure established and administered by a purely private organization or organizations, without direct government involvement

These governance options have different implications for the level of involvement of the Federal Government and stakeholders in the oversight, setting of policies, rules, standards, procedures, operational practices, liability/risk sharing, funding, and nature of compliance/enforcement within the SCMS industry.

From a Federal perspective, each option also may have certain pros and cons as it relates to authority, appropriations, safety, privacy, risk management, and continuity of operations. These are briefly summarized below. However, due in large part to the absence of Federal funds to support a public SCMS, DOT research on SCMS development to date has primarily focused on fleshing out a largely private model of SCMS governance. Based on this research, which has generated multiple examples of existing private sector governance organizations, we believe that a private model could be a viable mechanism for system governance of the SCMS. NHTSA's

existing legal authority will accommodate use of a grant, cooperative agreement, or other agreement to facilitate stakeholder – and even DOT -- input into governance of a private SCMS, assuming willingness on the part of the private entity to enter into such an agreement.

The VIIC, under a cooperative agreement with DOT, also has examined the viability of each of these models from industry's perspective, applying the following high-level principles, considered by its members as foundational for any governance entity:[270]

- Participation/voice,
- Accountability,
- Representation,
- Transparency,
- Efficiency,
- Flexibility, and
- Fairness and decency.

While it has not identified a preferred option, based on its governance work for DOT to date, the VIIC has taken the position that a private governance organization, without *any* government involvement (i.e., not under government contract, agreement or MOU), will lack sufficient authority to make all of the decisions and determinations necessary for appropriate system governance of the SCMS.[271] The VIIC also has expressed other concerns about a purely private governance model, including what it views as lack of stakeholder voice, accountability and government oversight; antitrust risks; potentially increasing costs; and "massive liability exposure."[272] The VIIC seems open to exploring various PPP models involving minimal "authority" passed on by NHTSA via contract, grant, cooperative agreement, MOU, or other agreement that would enable the SCMS Manager to conduct appropriate governance.

DOT will continue to use existing cooperative agreements with CAMP and the VIIC to further explore and develop SCMS governance models. Should NHTSA move forward with V2V regulatory action, additional research should include exploration of use of a private governance model (as the third option above), with some limited government involvement under

---

[270] In support of these principles, the VIIC cited the DOT June 2011 Governance Roundtable Proceedings (available at http://ntl.bts.gov/lib/43000/43100/43129/GovRoundtableProceedingsFINAL_9_22_11_v4.pdf, with Section 2.1 of the UNECE Guidebook on Promoting Governance in Public-Private Partnerships (2008).

[271] VIIC Assessment of Key Governance Policy Considerations for a Connected Vehicle Cooperative Safety Communications System – Part 1, delivered to DOT on March 13, 2013, at 9. See Docket No. NHTSA-2014-0022. Of specific concern to the VIIC are lack of authority to: (1) "compel universal participation"; "set or enforce rules applicable to external users and participants"; and "compel[ ] vehicle owners to maintain the ir vehicles in compliance with security protocols." VIIC, SCMS Organizational Policy Study, Interim Report, Dec. 11, 2012, at 16-17. See Docket No. NHTSA-2014-0022.

[272] Id.

an agreement with the private entity, assuming the entity's willingness to enter into such an agreement. This could facilitate stakeholder input into governance in the context of a privately owned/operated and governed SCMS, as this may be a variation on the private governance model that addresses some (albeit not all) of the VIIC's concerns about, and makes more palatable to industry the prospect of a privately owned, operated, and governed SCMS.

1. Public model

Under a public governance model, NHTSA would directly house or procure the SCMS system required to support deployment of V2V technologies. It most likely would do so through one or more service contracts with entities to serve as the SCMS Manager and CME component entities. Whether run by NHTSA or by NHTSA service contractors, the IT infrastructure and related business processes would be governed by Federal law, as appropriate, including but not limited to the Federal Information Systems Management Act, the Privacy Act, the Administrative Procedure Act, and the Federal Tort Claims Act. To the extent not already determined by applicable Federal laws, governance of the SCMS system would be NHTSA's direct responsibility, the specifics of which would be memorialized in NHTSA's contracts or agreements with its service providers. Such contracts or agreements would need to include specific provisions to ensure adequate market access, privacy and security controls, data rights, reporting, and continuity of services. Stakeholder input into governance of the security system would need to comply with the Federal Advisory Committee Act.

The FAA's air traffic control system is an example of a direct public governance model. It has a statutory basis, is funded largely by Federal appropriations, and its ownership, control, and operation are subject to Federal laws and procedures. As part of the air traffic control system, the FAA has a service contract (one of many with different private entities supporting its operations) with a private entity to provide data communications services for the NextGen program (including provision of the IT infrastructure required for NextGen communications -- but without such infrastructure becoming Federally-owned). The contractor has a nonexclusive legal right to consolidate and sell the data generated by the NextGen communications system. To the extent that it does so, the FAA receives a credit against reimbursed costs. The contract contains other provisions implementing Federal oversight and control, including oversight over security and data rights.

Currently, we believe that NHTSA has sufficient legal authority (under the Vehicle Safety Act and the "necessary expense" doctrine) , albeit insufficient appropriations, to enter into contracts related to the operation of the Security System required to deploy V2V technologies, if NHTSA were to regulate the V2V technologies in vehicles. Arguably, direct Federal operation or operation via service contracts would be the most effective mechanisms to ensure appropriate security, privacy, and long-term, stable continuity of operations, thereby reducing some of the more significant risks stemming from deployment of V2V technologies via an FMVSS dependent on a security system not directly regulated by the agency. However, absent substantial

new appropriations – which NHTSA has no plans to seek at this time – NHTSA lacks the resources to contemplate public ownership, control, or administration of a system the size and scope of the SCMS, as currently conceived. For this reason, DOT research to date has not fully explored a public governance model for the SCMS. Due to the current fiscal environment it does not seem plausible.

2. Public-private partnership model

Under a public-private partnership model, NHTSA would work with the private sector to form a Public Private Partnership (PPP) to operate and/or govern the security functions required to support deployment of V2V technologies. Depending on the scope of the agreement, the PPP could be limited to the SCMS Manager functions identified in the current CAMP/DOT security system model. Alternatively, the PPP could be responsible for owning, financing, and operating the Security System, as a whole, including the SCMS Manager and CME component entities. As yet another alternative, as discussed below, the PPP could be limited to forming a governance board of stakeholders to provide input, binding or not, to the SCMS owners/operators.

DOT and its stakeholders have identified multiple models of PPP entities to help inform our research on potential ownership, operation, and governance options for an SCMS. Examples include: publicly or privately owned utility models,[273] which are complex, highly regulated, and require significant public resources to administer: the Internet Corporation for Assigned Names and Numbers, which operates pursuant to an Memorandum of Understanding with the Department of Commerce that retains in DoD unilateral oversight for some functions and some but not all liabilities;[274] the End-of-Life Vehicle Consortium operated under MOU among the vehicle manufacturers, steelmakers, vehicle dismantlers, vehicle crushers, auto shredders, brokers, the environmental community, State representatives and the Environmental Protection Agency.[275]

Due primarily to a lack of current or foreseeable appropriations to support a PPP, DOT research to date has not fully explored development of a PPP governance model for the SCMS and, instead, has focused on a private model or ownership/operation and governance.

3. Private model

Consistent with our current resources, NHTSA has focused on working with stakeholders and DOT consultants to develop a viable model of private governance for the SCMS and its CME component entities. Ideally, the basis for the private oversight structure would be a

---

[273] Id. at 9-11.
[274] Id. at 4-6.
[275] Id. at 13.

coalition of CME component entities who, together, constitute and empower an SCMS Manager to decide on and enforce standards and processes applicable to the SCMS as a whole.

All organizations within the "industry," or all organizations that make up different parts of the SCMS environment, could be represented. The coalition of SCMS "industry" participants, together, could decide on standards, codes of conduct, expectations, and other norms in order to maintain and protect communications security, appropriate user privacy, and required operational functions within the system, under the auspices of the SCMS Manager and/or another coalition-type body. In addition, this group likely would decide on and participate in recommendations about resource management and costs for the industry and its governing body.

Many commercial industries today operate under this model of private governance, establishing private, industry-specific organizations to develop and enforce ethics, standards, code-making, and enforcement functions not specifically required by law. The largest benefit of this kind of governance structure is that it reduces the involvement of the government and therefore reduces the cost to the taxpayers for managing, administering, and enforcing rules within and across the CMEs, although the cost will be passed to the consumer at some point. It also provides more efficiency and flexibility in decision-making than typically is available in the context of a government or PPP model.

The positive and negative implications of a private governance structure include:

- Lower costs and more streamlined implementation/operational processes, due to the lack of Federal workplace regulations and processes
- Need for clear monitoring and enforcement standards and processes, potentially with an additional level of oversight or review/audit
- Need for agreements across jurisdictions, organizations, and areas of oversight so as to ensure smooth operations and reduced communications or collaboration challenges

The private model accommodates some limited Government involvement. Once a coalition or other private entity to serve as SCMS Manager is established voluntarily by a private SCMS "industry,"[276] NHTSA could enter into an agreement with that governance entity to ensure that SCMS functions required for V2V safety are delivered by CME entity organizations in a way that is consistent with DOT's Principles for a Connected Environment, discussed above -- and that such services are made available to all market participants in a secure, ongoing, nondiscriminatory, and privacy-appropriate manner. Such agreement also would provide the

[276] SIGNIFICANT CAVEAT: This governance analysis hinges on DOT successfully reaching a consensus agreement with a willing collation of OEM or another market participant to serve as SCMS Manager or otherwise ensure provision of the security system necessary for deployment of V2V technologies.

SCMS, as a whole, with the assurance that its activities would be, and would be perceived to be, in accordance with those principles.

Assuming willingness by the private entity to enter into such an agreement with the Government, either NHTSA or JPO authority might be used to support a mechanism for stakeholder input into SCMS governance, formal or informal. This kind of DOT-funded "governance" board is similar to what DOT envisions for governance of the NAS-owned SHRP2[277] databases: no Federal ownership or operation of the data but a group of interested stakeholders, including NHTSA and FHWA, on a governance board to establish high-level terms of access, security and privacy controls and similar aspects of operation.

Numerous real-world examples exist of organizations/systems in industries that self-govern through internal, binding contracts and agreements. Typically, such private governance is grounded in oversight and inter-organizational practices and agreements that provide the governing organization with adequate legal authority to establish and enforce industry-wide standards and maintain strong centralized functions, when appropriate. Often industries subject to self-governance also are subject to governance by local, State or Federal entities. Examples include:

- Aeronautical Radio, Incorporated (ARINC), the sole licensee for the airline communications frequency, is an example of a private governance organization identified by the VIIC, funded by membership and sponsorship annual dues.[278]

---

[277] The second Strategic Highway Research Program (SHRP 2) was authorized by Congress to address some of the most pressing needs related to the nation's highway system: the high toll taken by highway deaths and injuries, aging infrastructure that must be rehabilitated with minimum disruption to users, and congestion stemming both from inadequate physical capacity and from events that reduce the effective capacity of a highway facility. These needs define the four research focus areas in SHRP 2: (1) the Safety area is conducting the largest ever naturalistic driving study to better understand the interaction among various factors involved in highway crashes—driver, vehicle, and infrastructure—so that better safety countermeasures can be developed and applied to save lives; (2) the Renewal area is developing technologies and institutional solutions to support systematic rehabilitation of highway infrastructure in a way that is rapid, presents minimal disruption to users, and results in long-lasting facilities; (3) the Reliability area is developing basic analytical techniques, design procedures, and institutional approaches to address the events—such as crashes, work zones, special events, and inclement weather—that result in the unpredictable congestion that makes travel times unreliable; and (4) the Capacity area is developing a web-based tool to provide more accurate data and collaborative decision-making in the development of new highway capacity in order to expedite the provision of that capacity while simultaneously addressing economic, community, and environmental objectives associated with new construction. SHRP 2 is administered by the Transportation Research Board of the National Academies under a Memorandum of Understanding with the Federal Highway Administration and the America Association of State Highway and Transportation Officials. For more information, see www.trb.org/StrategicHighwayResearchProgram2SHRP2/Blank2.aspx (last accessed Jan. 30, 2014).

[278] VIIC, SCMS Organizational Policy Study, Interim Report, Dec. 11, 2012, at 15-16. See Docket No. NHTSA-2014-0022

- Payment Card Industry's governance via an agreement to adhere the Payment Card Industry Data Security Standard. Compliance with the 12 requirements of PCI DSS is necessary for merchants to be able to accept cards bearing the logos of the major payment card brands. The PCI Security Standards Council maintains PCI DSS, but enforcement of the standard is the responsibility of individual payment brands. The ATM Industry Association (ATMIA) is an independent, non-profit trade association that supports members of the ATM sub-industry through advocacy and education. Although critical for doing business, agreement to the PCI DSS is voluntary.[279]

Other than enforcement of those aspects of governance embodied in any agreement between the SCMS Manager and NHTSA, and any input provided via NHTSA's participation in a stakeholder board, as discussed above, under the private coalition model, NHTSA would play no further role in the self-governance of the SCMS "industry." The rules and obligations of industry participants would therefore depend on the entities that constitute and subject themselves to governance by the organization. A slightly different, potentially less inclusive (with regard to decision making) private governance model would result if an individual entity in the ITS marketplace, rather than a coalition group, agreed to serve as system manager overseeing the CME entities required for V2V safety; an individual entity could be an academic, State, or private (for profit or non-profit) organization. Either private governance model could be supplemented by a stakeholder "governance board" to establish or suggest policies and practices for the SCMS Manager to apply system-wide, to the extent that the private CME owners/operators agree to consider or be bound by such input.

With a private system owner/operation, ultimately, the details of internal governance (like the details of internal organization) would be up to that private CME entity/entities – in particular, the entity serving as SCMS Manager -- and the Federal Government's role would be limited to ensuring that entities honored the terms of their agreement with DOT or NHTSA, if an agreement exists. As noted above, that DOT agreement primarily would include a provision that the private SCMS's delivery of security functions required for V2V communications would be consistent with DOT's Principles for a Connected Environment, provide adequate market access, incorporate appropriate protection of privacy and security, and involve reporting and sufficient continuity of services obligations to ensure the long-term stability and availability of the SCMS. However, as noted above, the private model could be supplemented with a stakeholder governance board to advise on governance issues that NHTSA or JPO likely could support under a cooperative agreement or grant for that limited purpose.

---

[279] BAH SCMS Design and Analysis Report, at 35-36. See Docket No. NHTSA-2014-0022

While the private model possesses considerable benefits, it also carries certain risks that the Federal model does not. The primary risk of a purely private model involves continuity of SCMS function. With no Federal involvement, the party or parties owning and operating the SCMS theoretically could choose to stop doing so at some point. A V2V system needs an SCMS to function; if the SCMS owner/operator ceases to provide the security required for V2V communications, the V2V system will no longer work. Even with some amount of Federal involvement, it remains difficult to compel specific performance if the performing party chooses to stop performing. One option for minimizing the not insignificant risk associated with a private model, should NHTSA enter into an agreement with a private SCMS owners/operator, is to include certain contractual provisions in the agreement. NHTSA can structure the agreement so that the private SCMS owners/operator is required to provide sufficient notice of its intent to cease providing V2V security services and to continue operating the SCMS until NHTSA can identify another entity to assume operations, or so that the Federal Government receives liquidated damages in the event of non-performance. Of course, "lights out" also could be a risk under a Federal model if Congress suddenly withdraws funding after NHTSA establishes the SCMS. In any event, a thorough consideration of contingencies for risks such as this seems highly advisable.

4. Scope of the SCMS system governance

In order to define governance policy, it is first necessary to identify the SCMS functions that need governing in order to deploy V2V technologies, and why. Please note that there may be Federal, State, and local laws applicable to various areas discussed below as appropriate for governance. Where relevant, we have attempted to identify the applicable legal authority. However, as used in this discussion, the term "governance" focuses primarily on those aspects of the SCMS and SCMS activities *not* already addressed by existing laws.

To set the stage for this analysis, following is a brief summary of the industry perspective on governance needs, as represented by the VIIC,[280] and of NHTSA's somewhat different perspective.

a) The VIIC perspective

Pursuant to a cooperative agreement funded by DOT, the VIIC has provided to DOT a series of white papers summarizing their members' consensus views on various policy issues relating to V2V technologies. Also pursuant to that agreement, the VIIC has provided policy support to CAMP in its development of the technical and organizational/operational designs for the SCMS. As detailed above, CAMP has designed and the VIIC views the SCMS as a collection

[280] DOT funded the VIIC's research specifically to obtain industry's views on V2V policy issues such as privacy, liability, SCMS governance and data ownership.

of functions consisting of multiple organizational groups, specifically, a central SCMS Manager and central and non-central CME component entities.[281] Unlike DOT consultants, the VIIC does not regard as problematic a single CME entity conducting functions that are both central and non-central in nature, as long as select functions reside in separate legal entities. The VIIC sees a pressing need for a single SCMS Manager with governance authority over the CME component entities and the functions that make up the SCMS, listed above.

The mission of the SCMS Manager would be to:

- Set SCMS organizational structure
- Establish operational rules and processes
- Define means of separation of functions
- Provide mechanisms for certification, audit, enforcement and adjudication
- Establish funding mechanisms
- Provide adequate risk management, and
- Have ability to address cross-border issues

The VIIC has indicated that certain key functional areas, both outside and inside the SCMS, require the oversight, control and consistency of governance, Table IX-3[282]

Table IX-3 VIIC Concept of Security Certificate Management System Functional Area Distribution

Functions outside of the SCMS:	**Functions Within the SCMS:**
Performance requirements and standards (to be established by NHTSA FMVSS)	Security system (SCMS) internal operations and management Rules of operation and maintenance Rules of use and access to the SCMS for devices beyond V2V safety
Device certification and enforcement (under an FMVSS and the Motor vehicle Safety Act)	Device security interoperability
What messages and broadcast on what channels (FCC/NTIA/Spectrum Manager)	Privacy
Device communication interoperability (FCC/FMVSS)	Device certification with the SCMS
Spectrum Management (FCC/NTIA/Spectrum Manager)	Cross-border acceptance and international harmonization
Data access and ownership – usage, security and privacy*	Oversight/administrative functions
Liability Risk Management*	Funding

*According to VIIC but not NHTSA

[281] VIIC Assessment of Key Governance Policy Considerations for a Connected Vehicle Cooperative Safety Communications System – Part 1, at 16 (delivered to DOT on March 13, 2013). See Docket No. NHTSA-2014-0022.
[282] Id. at 10 *et seq.*

The VIIC has suggested that the functional areas falling outside of the SCMS, listed above, are those that likely will be governed by an FMVSS, the Motor Vehicle Safety Act, a spectrum manager, or other standards or entities.[283] The additional notes in parentheses identifying the likely sources of external governance outside of the SCMS that did not originate from the VIIC but were added by NHTSA for purposes of clarity.

b) NHTSA perspective

NHTSA generally agrees with the VIIC's characterization of the functions that need governance outside of the SCMS, with two significant exceptions marked by asterisks in the left column of the VIIC chart above: data access and ownership, and liability. To the extent not already addressed by existing Federal, State, and local law, we see data access and ownership to be squarely *within* the scope of the SCMS's governance of privacy and intellectual property/data rights through its Privacy Policies – not as an external function. Placement by the VIIC of access/ownership and privacy outside of the SCMS is, however, consistent with the VIIC's previously-expressed position that data access/ownership and privacy should be the subject of new Federal legislation and regulation designed to implement stringent restrictions on access to and use of BSM data broadcast by OBE. The VIIC position is grounded in the OEMs' concern that inadequate privacy protection will adversely affect consumer acceptance of V2V technology and, ultimately, new car sales. NHTSA understands that concern but believes privacy can adequately be protected through the SCMS.

A second area that NHTSA does not see as needing active or new forms of governance outside of the SCMS is that of liability/risk management. In our view, the liability of participants in the envisioned V2V warning system already is governed by existing Federal, State, and local laws and legal authority, including but not limited to those establishing tort/product liability for government and non-governmental entities and individuals.[284] The VIIC and NHTSA agree that how risk is allocated *within* the SCMS would be a matter for internal governance under the auspices of the system manager function.

NHTSA also agrees with CAMP and the VIIC about the key functional areas within the SCMS that will require the oversight, control, and consistency of a sole, central internal governance structure. In our view, the critical SCMS functional areas that will need internal governance and management are:

- **Organizational Structure/Ownership**: requirements for functional separation/groupings and expertise/viability requirements

---

[283] Id. at 12.
[284] Section X.

- **Operational Policies and Processes:** mechanisms for certification, audit, enforcement, and adjudication
- **Interoperability**: standards for device communications and security interoperability
- **Security/Privacy Assurance**: certificate policy, including physical, procedural, and technical controls
- **Privacy/Data Ownership Policy:** a policy applicable CME-wide that protects individual privacy and data that can be linked appropriately to an individual

However, we note that the latest SCMS design refers to the central internal management function as the "SCMS Manager." For consistency, throughout this discussion we, too, use the term SCMS Manager to refer to the function that would undertake internal operations and management of the CME component entities by providing policy and technical standards for the entire CME "industry." The SCMS Manager function could be carried out a number of different ways. As is often the case in large commercial industries, a volunteer industry consortium could take on this role. In other industries, or in public or quasi-public industries, a regulatory agency or other legal or policy entity often performs the central management role. In the context of the SCMS, we expect that a single legal/administrative entity will take on the SCMS Manager role – but, as noted above, that entity could function with input from a "governance board" funded by DOT via a cooperative agreement or grant, assuming available funds, if the private SCMS Manager entity consents to accepting such input on an advisory or ideally a binding basis.

X. Legal Liability

A. Overview

Legal liability is a policy issue frequently identified by industry -- and to a lesser extent by other stakeholders -- as a potential impediment to deployment of V2V technologies. The Federal Government has multiple available tools to limit legal liability, when Congress deems it appropriate to do so. If NHTSA moves forward with regulating V2V technologies, the agency will need to work with the Department to determine whether to support liability limiting or sharing mechanisms that would limit the legal exposure of industry, some or all parts of the SCMS, or potentially other stakeholders. However, ultimately, it will be up to Congress to determine whether such liability limiting mechanisms are appropriate in the context of V2V communications.

The decision options currently under consideration by NHTSA involve safety warning technologies -- not control technologies.[285] As discussed below, from a products liability standpoint, V2V safety warning technologies, analytically, are quite similar to on-board safety warnings systems found in today's motor vehicles. For this reason, NHTSA does not view V2V warning technologies as creating new or unbounded liability exposure for industry. The agency, therefore, does not see a current need to develop or advocate the liability limiting agenda sought by industry in connection with potential deployment of V2V technologies via government regulation.

One factor that will contribute to NHTSA's assessment of the degree to which liability could be an impediment to development of a private SCMS is the extent to which the primary and secondary insurance markets make insurance coverage available to CME entities. Another factor will be the extent to which CME entities are able to limit their legal liability via terms of use or similar contractual mechanisms applicable to individuals or entities participating in the connected vehicle environment.

B. Industry's liability concerns and solutions

Throughout the V2V research process, DOT has accessed information about the positions of industry members on various V2V policy issues two primary ways: (1) through a cooperative agreement between JPO and the VIIC designed specifically to obtain industry's views on various

---

[285] To the extent that future regulatory action by NHTSA contemplates requiring safety control technologies, NHTSA will revisit the appropriateness of advancing liability limiting measures protective of industry and/or other stakeholders.

policy issues, and (2) through discussions with individual industry members. While the following discussion of liability references primarily the positions and views expressed by the VIIC, the concerns expressed informally by individual OEMs and manufacturers to DOT officials have been largely consistent with that of the VIIC. Not surprisingly, industry is worried that deployment of V2V technologies may increase its liability exposure.

The VIIC readily has acknowledged that manufacturers regularly address risk management as an integral part of designing and manufacturing vehicles for the real world.[286] However, it has suggested that cooperative crash avoidance safety applications present an "unprecedented challenge to risk management."[287] VIIC's position has been that "the design, development of ultimate deployment of DSRC-based V2X communications systems creates unique risk allocation concerns among the wide range of partisans (both public and private sector)" and that risk allocation is "further complicated by the introduction of aftermarket devices, the potential for system tampering/hacking, and the risk of unauthorized access to networks and to sensitive data."[288] As stated by VIIC, it may be difficult to determine who is liable for a V2V system failing to perform as the driver expected, due to the complexity of the system and the number of parties involved.[289] The VIIC also has noted that a NHTSA regulation promulgated under the Safety Act would not provide industry with adequate risk management because such regulations do not expressly preempt common law tort liability.[290]

In support of its position, the VIIC has compared DSRC communications designed to enable low-latency safety applications to convenience services provided over commercial wireless networks.[291] It concluded that "the potential risk implications for low latency safety warnings are substantially higher than exist today for convenience services."[292] The VIIC's liability assessment seems to be based, in large part, on the expectation that there will be no contract allocating risk among individuals and entities involved in the V2V environment. In the context of convenience services, such contracts control the relative distribution of risk among the multiple entities involved in providing services. By contrast, as envisioned by CAMP and the VIIC, presumably participants in a mandatory V2V safety system would not be required to enter into contracts with the security or communications service providers or other participants. In the

---

[286] White Paper on Risk Management Issues, Vehicle Infrastructure Integration Program, VIIC Deployment Analysis and Policy Work Order #4, Task 13 General Policy Support, at 2 [Hereafter, "VIIC Risk Management White Paper"], delivered to DOT on 4/18/2012. See Docket No. NHTSA-2014-0022.
[287] VIIC Risk Management White Paper, at 2.
[288] Id., at 1.
[289] Task 14 Aftermarket Device Research Addendum (06-30-2010 v3) p. 54, Nov. 8, 2011.[Need Docket #]
[290] VIIC, SCMS Organizational Policy Study, Interim Report, Dec. 11, 2012, at 2. See Docket No. NHTSA-2014-0022
[291] Risk Management White Paper, at 1.
[292] Id.

VIIC's view, there would be no contract, legal mechanism, or case law to provide courts with guidance on risk allocation.[293]

In addition to the lack of contractual limitations and legal precedent, other primary liability issues identified by the VIIC[294] include:

- Whether and, if so, how V2V warning applications increase the risk of liability for OEMs, operators, and drivers;
- The need for Congress to put in place one or more legal mechanisms for distributing risk among OEMs, operators, drivers, and other public and private stakeholders;
- Whether V2V warning applications will change the way the legal system assesses driver versus equipment error;
- Whether owners may be held legally accountable for shutting off or failing properly to maintain V2V warning systems; and
- Whether the human machine interface required for V2V warning systems will increase driver distraction in a way that will affect legal liability.

The VIIC has identified as examples of Federal liability limiting mechanisms preemption (explicit or implied), immunity (as with 911 services), indemnification (for Federal contractors), and other types of limitations on damages or ways to allocate risk to government and away from industry (other examples of which are detailed in a risk assessment report prepared by the Dykema law firm for the VIIC[295] under the JPO cooperative agreement).[296] The VIIC also has noted that "the nature and extent of desired liability protections will depend on the governance model chosen and reasonably anticipated legal risks."[297] VIIC has asserted that the greater the involvement of the government, the less likely it is that the SCMS's activities will be challenged or exposed to liability for harm to property or persons.[298] In discussions, both the VIIC and some specific industry members have tied their support for deployment of V2V safety technologies to the Federal Government's willingness to put in place liability limiting mechanisms. However, NHTSA does not believe this is a uniform industry position, in that not all OEMs consider liability protection as a condition precedent to going forward with V2V implementation.

---

[293] Id.
[294] Id., at 2.
[295] Dykema, Risk Assessment Report, under contract to VIIC (Policy work order, Task 6, Deliverable 1), Mar. 12, 2009, at 38-65. [Hereafter, "Dykema Risk Assessment Report"]. See Docket No. NHTSA-2014-0022.
[296] VIIC, SCMS Organizational Policy Study, Interim Report, Dec. 11, 2012, at 19. See Docket No. NHTSA-2014-0022
[297] Id.
[298] Id., at 26.

C. Liability concerns specific to the SCMS

Specifically with respect to the SCMS, the VIIC has indicated that it views liability risk management within the SCMS as a key functional area requiring internal governance.[299] The VIIC identified the SCMS Manager as the entity with responsibility not only for *governing* liability risk management within the SCMS but also for *providing* liability risk protections to all CME entities making up the SCMS.[300] The VIIC has taken the position that the Federal Government will need to grant to the SCMS broad governance authority (through statute, Executive Order, regulation, contract, or other means) – possibly cross-border authority -- and has stated that the mechanism through which legal authority is conveyed could provide liability protections for central or non-central SCMS elements.[301]

D. Federal liability limiting mechanisms

The Federal Government has at its disposal a range of mechanisms to limit the liability of private and public entities and individuals, when Congress deems it appropriate. Some examples of liability limiting mechanisms include:

- **Explicit/Implicit Preemption**, e.g., under the Federal Motor Vehicle Safety Act;
- **Contractual Indemnification via contract or agreement**, e.g., indemnification for contractors providing hardware and software to update the FAA's air traffic control system under its En Route Traffic Computer Replacement Program; Public Law 85-804, the indemnification authority primarily used by the Department of Defense;
- **Statutory Immunity,** e.g., Federal Volunteer Protection Act, extending immunity protections to volunteers affiliated with non-profits provided they do not receive compensation in excess of $500 per year;
- **Capped Liability,** e.g., Amtrak Reform and Accountability Act of 1997, limiting overall damages from passenger claims to $200 million from a single railway incident and explicitly authorizing passenger rail providers to enter into indemnification agreements; Oil Pollution Act of 1990, passed after the *Exxon Valdez* accident, making oil companies responsible only for the first $75 million of liability claims from businesses and organizations affected by a spill; and
- **Risk Transfer, Insurance Pools, and Reinsurance Programs**, e.g., Price-Anderson Act, providing for two-level insurance pool covering nuclear power industry;

---

[299] VIIC Assessment of Key Governance Policy Considerations for a Connected Vehicle Cooperative Safety Communications System -- Part 1, at 5 (Mar. 12, 2013). [Hereafter, "VIIC Governance Paper"]. See Docket No. NHTSA-2014-0022.
[300] Id., at 15 and 20.
[301] Id., at 19.

Commercial Space Launch Act of 1984, requiring insurance up to 500 million cap with 500 million to 1.5 billion in coverage provide by Federal Government.

These are just a few examples of liability limiting or risk shifting mechanisms. Many such programs are hybrids created to address specific catastrophic risks or to encourage development and/or deployment of new technologies.

All such programs require Congressional approval. The question for NHTSA is whether public and private entities that may be involved in provision of V2V communications, including but not limited to the OEMs, will agree to move forward with deployment of V2V communications if DOT does not seek and Congress does not approve some form of liability limiting/risk sharing program.

E. NHTSA's assessment of industry liability

Will industry concerns about liability be a stumbling block to regulation of V2V technologies? We think not – at least not to the dramatic extent that some industry stakeholders have suggested.

Under traditional product liability tort law theories,[302] OEMs will be responsible if they manufacture and sell a defective product that causes harm to a person or property.[303] This includes liability for design defects, manufacturing defects, and defects due to inadequate warnings.[304] According to one legal analysis, there are a number of different potential product liability claims that could be associated with V2V technologies.[305] As stated above, the VIIC has suggested that it may be difficult to determine who is liable for a V2V system failing to perform as the driver expected, due to the complexity of the system and the number of parties involved.[306]

However, the V2V technology currently under consideration results in safety warnings - not motor vehicle control. For this reason, ultimately, it is the driver who remains responsible for failing to avoid a crash. It will be difficult for a driver to prove that an accident would have been avoided had the V2V system functioned properly. Potential liability based on V2V defects,

---

[302] Product liability laws vary from State to State, but a good overview of the relevant common themes in State product liability tort law is set forth in the Dykema Risk Assessment Report, at 21-34.
[303] Restatement (Third) of Torts Ch. 1 § 1.
[304] Restatement (Third) of Torts Ch. 1 § 1.
[305] The Dykema Risk Assessment Report identified four groups of likely product liability claims stemming from to V2V: (1) OEM failure to deploy V2V; (2) improper installation or location of technology; (3) failure to maintain OBE; and (4) claims associate with operation and use of OBE, including OBE failures and claims involving operator-OBE interaction.
[306] Task 14 Aftermarket Device Research Addendum at 54 (06-30-2010 v3, Nov. 8, 2011). See Docket No. NHTSA-2014-0022

therefore, will be limited substantially by lack of causation due to drivers' roles in failing to avoid crashes.

A lawsuit also might allege that a crash was caused, in whole or in part, by a failure in the communications infrastructure supporting V2V (e.g., an RSE). However, as evidenced by the numerous lawsuits claiming that failure of a traffic light contributed to an accident, such cases typically are brought against public or quasi-public entities and not against vehicle manufacturers.[307] For this reason, we would not expect alleged failures in V2V infrastructure to impact OEM liability in a significant way.

Significantly, V2V safety warnings are not very different in terms of application or interaction with the driver than on-board safety warning systems found in many of today's motor vehicles. Under the existing product liability tort law framework, manufacturers have the ability to take steps to limit their legal liability stemming from such on-board systems through a variety of mechanisms (e.g., compliance with applicable safety standards, contractual indemnification by OBE suppliers, dispute resolution/arbitration clauses applicable to supplies and consumers[308]). One important mechanism is provision by the OEM of adequate consumer warnings and instructions for using V2V equipment. Such consumer warnings and instructions would emphasize the limited role of V2V safety warning technology and explain the limitations of the system in the foreseeable operating environment.[309] As specifically noted in the Dykema Risk Assessment Report:

> This approach does not call for a new or unprecedented effort. Newer vehicle models currently on the market that are equipped with systems such as lane-departure warning, backover detection warnings, and forward vehicle detection typically follow this approach in carefully describing the operation and limitation of these systems.
>
> We would expect that manufacturers would follow this same approach to limiting their potential liability in connection with V2V warning systems.[310]

F. NHTSA's assessment of SCMS liability

Will industry concerns about liability be a stumbling block to creation and operation of a private SCMS "industry?" For the reasons discussed below, we think probably not – and certainly not to the extent suggested by the VIIC and certain members of the industry.

---

[307] Dykema Risk Assessment Report, at 33.
[308] Dykema Risk Assessment Report, at 34-38.
[309] Dykema Risk Assessment Report at 35 ("these systems differ from traditional technologies because of the manner and degree of interdependence on systems outside the host vehicle (other vehicles, RSEs, communications systems) and also because they may be affected by roadway, environmental, and other variables over which the OEM has little or no control").
[310] Id.

As discussed elsewhere in this report, to date, NHTSA has focused on a private model of SCMS governance that would not involve Federal funds or a Federal grant of formal legal authority to the SCMS or SCMS Manager -- but instead would result from the CME entities themselves agreeing to "self-governance" by a central SCMS Manager pursuant to binding contracts or agreements. Such industry self-governance by an SCMS Manager likely would involve the SCMS Manager establishing minimum insurance requirements and/or negotiating, on behalf of members, for system-wide insurance coverage. The SCMS Manager also might work with the CME entities to determine the appropriate distribution of liability for harm. However, the SCMS Manager would not necessarily be the entity responsible for *providing* liability protection to individual CME entities, whether central or non-central, as has been suggested by the VIIC. Unless the SCMS Manager worked with the CME entities to distribute risk among participants in a way that provides indemnity to some entities, the agency presumes that individual CME entities would carry liability insurance sufficient to ensure adequate coverage, in accordance with the insurance requirements established by the SCMS Manager.

The agency also anticipates that any contract or agreement between NHTSA and the SCMS Manager and/or SCMS entities would be limited primarily to ensuring adequate system security and privacy, periodic reporting, and ready access to information need by NHTSA to investigate and recall defective vehicles or V2V equipment. Additionally, at this time NHTSA does not see the need for a formal grant of legal authority to a private SCMS, either with or without some form of contractual liability limitation.

As discussed above, the V2V technology under consideration results in safety warnings - not motor vehicle control – and, ultimately, it is the driver who remains responsible for failing to avoid a crash. For this reason, it will be difficult for a driver to prove that an accident would have been avoided had the SCMS security system functioned properly. Potential liability based on failures in the SCMS, therefore, will be limited substantially by lack of causation due to drivers' roles in failing to avoid crashes. It also is not clear to the agency why an SCMS Manager could not require that individuals and entities participating in an SCMS agree to terms of use that would limit the liability of the SCMS and its component entities, either explicitly or via the same type of instructions and explanations of system limitations that the OEMs would use to limit liability.

Additionally, the automotive industry seems to have significant incentives to help stand up and operate several elements of the SCMS, as currently designed, including the RA and SCMS Manager. As the only outward facing component of the SCMS, the RA is critical to the ability of individual OEMs to maintain control over its customer relationships. As the entity charged with establishing and enforcing policies and procedures applicable to all CME entities making up the SCMS, the SCMS Manager presumably will promulgate policies directly implicating the financial interests of OEMs and other manufacturers, such as liability distribution and intra-CME fees (i.e., the costs to motor vehicle and device manufacturers of obtaining certificates and certificate-related services (e.g., device type certification and bootstrapping)).

While the organizational structure of the SCMS will need to be consistent with anti-trust laws and sound conflict of interest principles, the VIIC's governance deliverables to date consistently have reflected industry's interest in having a strong voice in SCMS governance (which, in the context of the CAMP SCMS design, means a strong voice in the operation of the SCMS Manager). Industry's voice in governance cannot be assured unless it plays a significant role in standing up and operating a private SCMS.

Nevertheless, the agency believes that it is premature to take a position on the need for liability limiting mechanisms applicable to some or all CME components of the SCMS in order to encourage the establishment and operation of a private SCMS to provide security for V2V communications. As noted by the VIIC, the appropriateness of such liability limiting/risk sharing measures will turn on the constitution and governance of the SCMS. Another factor affecting NHTSA's assessment of whether liability could be a stumbling block to development of a private SCMS will be the extent to which the primary and secondary insurance markets will make insurance coverage available to CME entities.

XI. Preliminary Cost Estimates of V2V Implementation

A. Overview of preliminary estimated V2V costs and benefits

The preliminary estimates explored in this and the following sections are based on currently emerging, prototype V2V technologies and existing data. The agency would expect these estimates to be revised when more advanced technologies and additional data are available for inclusion in an analysis. This and the following sections on benefits and cost-effectiveness are considered a minimal analysis of three potential scenarios with current, prototype V2V technology. The agency would need to conduct a more comprehensive regulatory impact analysis if there was a need to support any such action.

This section details the process of how the agency estimated preliminary costs for potential V2V technology deployment. The following section, Section XII, describes the preliminary benefit analysis.

The preliminary cost and benefit estimates are provided for three pre-determined technology implementation scenarios. These estimates provide a wide range of cost and benefits of a potential V2V implementation. The cost in this analysis comprises four categories: vehicle equipment, fuel economy impact, communications costs, and SCMS. Together, we estimate that the total cost per vehicle to the consumer for each vehicle will be approximately $341 to $350 in 2020 (across the 3 percent to 7 percent discount rates and three scenarios). This amount is projected to decrease over time to an approximate range of $209 to $227 by 2058. Of the four cost categories, the initial vehicle component cost is estimated separately for new vehicles and old vehicles. The component cost is $329 per new vehicle in 2020, and it will decline progressively to $186 to $199 in 2058. The fuel economy impact is estimated to be $9 to $18 per vehicle. The communications costs range from $3 to $13 per vehicle, with an average cost of $8.30 to $8.50. The component cost (i.e., aftermarket safety devices) per old vehicle range from $160 to $387. The SCMS costs range from $1 to $6 per vehicle with an average of $3.14. The SCMS cost will increase over time due to the need to support an increasing number of vehicles with the V2V technologies.

The total preliminary annual costs (the sum of the four categories of costs) of the V2V system fluctuates year after year but generally show a declining trend. The estimated total annual costs range from $0.3 to $2.1 billion in 2020 with the specific costs being dependent upon the technology implementation scenarios and discount rates. The costs peak to $1.1 to $6.4 billion between 2022 and 2024, and then they gradually decrease to $1.1 to $4.6 billion.

B. Discussion of V2V preliminary cost estimates

Based on the agency's preliminary assessment, the total annual costs of the V2V system will vary substantially from year to year. In addition to the on-board equipment (OBE) costs of a V2V system (i.e., the components that need to be installed on a vehicle to support the V2V safety applications operating in the system), there are also costs for fuel economy impacts, the SCMS, and communication between the SCMS and OBEs. These cost estimates are highly influenced by the technology implementation pace. Therefore, the agency used three different implementation scenarios (i.e., the rate at which new vehicles and aftermarket devices are purchased each year) to illustrate the potential total costs and the annual impact of establishing a V2V system. These three scenarios range from an aggressive implementation schedule that includes aftermarket devices and 100 percent implementation for new vehicles in three years, to a relatively slower implementation schedule that does not have aftermarket devices and with a maximum of 25 percent of full implementation. Across the three scenarios and two discount rates (3 percent and 7 percent), the estimated total costs rise from $0.3 to $2.1 billion in 2020 to a total of $1.1 to $6.4 billion in 2022, and gradually decrease to a relatively stable level of $1.1 to $4.6 billion.

Breaking down those annual cost estimates, NHTSA currently estimates, based on our preliminary information, that the on-board equipment necessary to support the V2V safety applications would cost $329 per vehicle in 2020, with the possibility that these costs will decrease over time as manufacturers gain experience producing this equipment (a phenomenon known as the "learning curve"). Given the various sales scenarios considered, we believe that the price per vehicle could be as low as $260 in 2022 and $186 in 2058, as discussed in more detail below.

In addition to the cost of purchasing/installing the V2V equipment, there are fuel economy costs due to the weight of the V2V equipment. The agency estimated that V2V equipment will increase each vehicle's total weight by approximately 3.45 pounds. Consequently, it will increase fuel costs by between $9 and $12 for passenger cars over the lifetime of the vehicle, and $11 to $18 for light trucks.

The next cost category is the secure communications cost which is the cost of ensuring secure communications between vehicles and the SCMS and among the SCMS operations. For the first 3 years, based on our assumptions about certificate issuance and delivery, no communications will occur to renew certificates. Further, due to the low overall V2V penetration rate among the operational vehicles, the agency believes that the probability of misbehavior is extremely low and thus the need for a secure communication is not critical. There are, therefore, no communication costs for the first three years. In year 4, the average per-vehicle cost to pay for communication is estimated to be $8.58 to $10.74, with the price potentially as low as $3.37. At its peak, the per-vehicle cost increases to $12.39 to $12.97, with an average fee that could be charged to vehicles sold from year 4 through the next 37 years ranging from $8.30 to $8.50.